Научная статья
УДК 004; 519
doi: 10.34987/vestnik.sibpsa.2024.51.59.010

Синтез корпоративной системы повышения уровня осведомленности персонала в области информационной безопасности

Максим Юрьевич Синещук

Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия
Автор ответственный за переписку: *Максим Юрьевич Синещук, smaxim@igps.ru*

Аннотация. Представлен методический аппарат для управления развертыванием в действующей организационной системе сервисов обучения персонала навыкам кибербезопасности на базе корпоративной информационной инфраструктуры, системы обеспечения информационной безопасности и современных технологий киберполигона с целью повышения уровня осведомленности о киберугрозах, методах атак, способах и средствах защиты.

Ключевые слова: синтез организационной системы, осведомленность, информационная безопасность, киберугрозы.

Для цитирования: Синещук М.Ю. Синтез корпоративной системы повышения осведомленности персонала по информационной безопасности //Сибирский пожарно-спасательный вестник. 2024. № 1(32) . С. 88-96. https://doi.org/ 10.34987/vestnik.sibpsa.2024.51.59.010

Благодарности: работа выполнена по государственному заданию МЧС России прикладных научных исследований по темам «Киберсреда» и «Гармония» в Санкт-Петербургском университете ГПС МЧС России, автор выражает особую благодарность научному руководителю Богдану Васильевичу Гавкалюку и кафедре прикладной математики и информационных технологий за помощь при подготовке статьи.

Original article

SYNTHESIS OF A CORPORATE SYSTEM FOR RAISING STAFF AWARENESS IN THE FIELD OF INFORMATION SECURITY

Maxim Yu. Sineshchuk

Saint-Petersburg University of State Fire Service of EMERCOM of Russia, Saint Petersburg, Russia
Corresponding author: *Maxim Yu. Sineshchuk, smaxim@igps.ru*

Abstract. The methodological apparatus for managing the deployment of cybersecurity training services in the current organizational system based on corporate information infrastructure, information security systems and modern cyberpolygon technologies in order to increase awareness of cyber threats, attack methods, methods and means of protection is presented.

Keywords: synthesis of the organizational system, awareness, information security

For citation: Sineshchuk M.Yu. Synthesis of a corporate system for raising staff awareness in the field of information security // Siberian Fire and Rescue Bulletin 2024. № 1 (32). C. 88-96. https://doi.org/ 10.34987/vestnik.sibpsa.2024.51.59.010

Acknowledgements: I express special gratitude for the help in preparing the article to the scientific supervisor Gavkalyuk Bogdan Vasilyevich and the Department of Applied Mathematics and Information Technologies of St. Petersburg UGPS of the Ministry of Emergency Situations of Russia.

Введение

Развитие киберугроз и усиление кибератак на информационную инфраструктуру (ИИ) предприятий на фоне цифровой трансформации реального сектора экономики изменили отношение к защите информации, совершенствованию правовой базы (федеральные законы: № 149-ФЗ, № 152-ФЗ, № 187-ФЗ), регламентации организационно-технических мер по обеспечению безопасности информационных технологий (ИТ), ресурсов и данных, включая персональные (Приказы ФСТЭК России № 17, № 21, № 31, № 239; ГОСТ Р серии 2700х, 50922, 51275, 52069.х, 53114, 56045, 57580.х, 59382, 59407, 59547; СТО типа БР ИББС, Газпром 4.2-0-003).

Деятельностное участие персонала в цифровой производственной среде, новые в цифровой экономике трудовые функции и риск некомпетентных действий обусловили необходимость выработки и внедрения в существующие корпоративные системы интерактивных сервисов непрерывного обучения и оценки полученных навыков по результатам повышения уровня осведомленности в области информационной безопасности (ИБ) [1].

На практике используются различные варианты корпоративных архитектур посредством внешнего компонента - облачных сервисов специализированных операторов, например, Kaspersky ASAP, платформ фишинга (ООО «Фишман»; ООО «Ростелеком-Солар», см. Рис. 1), выделенного корпоративного специализированного компонента (АНО ДПО «Корпоративный университет Сбербанка»; АНО «Корпоративная Академия Росатома», см. стек программ обучения Рис. 2) или интегрированного компонента действующей инфраструктуры (модуль интеграции систем обучения и технической учебы АО «РЖД»).

Новой, наиболее сложной и актуальной является организация интегрированного компонента с применением перспективных образовательных технологий.

Рис. 1. Архитектура сервисов платформы «Ростелеком-Солар»

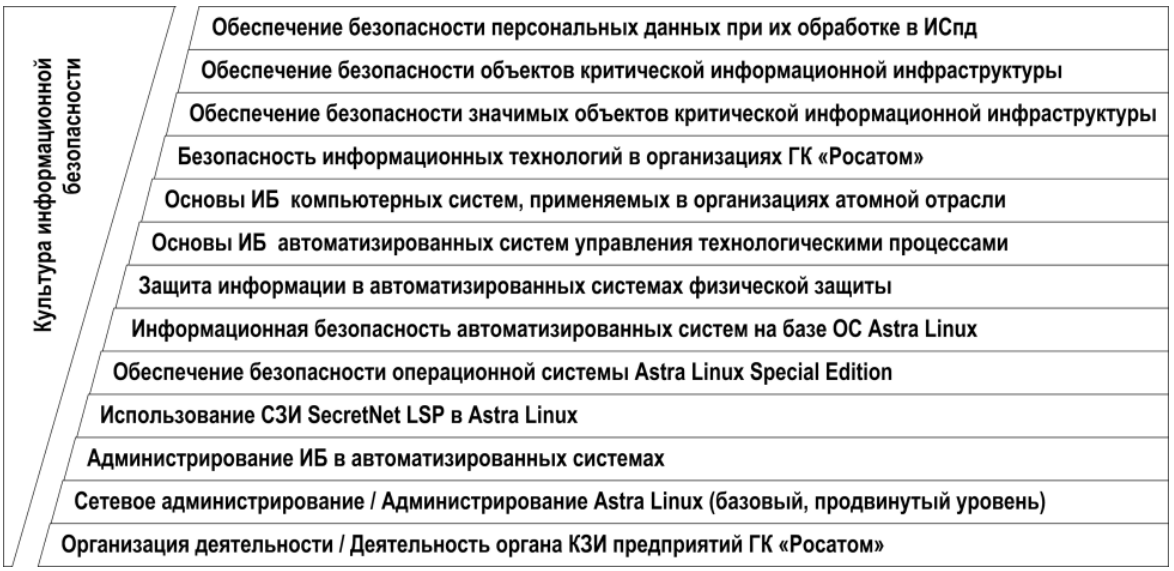

Рис. 2. Архитектура сервисов программ обучения Академии Росатома

Перспективные сервисные образовательные технологии в области информационной безопасности и их процессное описание

Перспективной образовательной технологией в области ИБ является киберполигон (КП). Отечественный рынок КП бурно развивается с учетом опыта эксплуатации зарубежных программных средств. Сегмент отечественных компаний ограничен и является устойчивым (АО «Центринформ», ЗАО «Позитив Технолоджиз», ЗАО «Перспективный мониторинг», ООО «Солар Секьюрити» и другие). Применение КП направлено на совершенствование корпоративной системы обеспечения ИБ за счет формирования непрерывной проактивной киберсреды на принципах экосистемы. Корпоративные КП и их субъекты предназначены для предметно-ориентированного непрерывного обучения в области ИБ, организации прикладных исследований технологий кибербезопасности, информационной поддержки подразделений системы управления ИБ.

Совокупность организационных, функциональных, информационных и технических ресурсов субъектов КП с набором сервисов для конкретной целевой задачи (кибертренировки (киберучения), обучения, исследования) называется треком (ТК, ТО, ТИ). Перечень типовых сервисов треков КП, например ТО, содержит:

- сервисы профориентированного образования по направлению ИБ с применением компьютерно-моделирующей среды прототипов и цифровых двойников реальных фрагментов корпоративной ИИ;
- сервисы формирования, апробации и внедрения новых дидактических методов с применением территориально-распределенных средств КП и виртуальных сред;
- сервисы формирования и регламентированного функционирования проактивной киберсреды информационной поддержки в корпоративной системе управления ИБ по проблемам текущей деятельности профильных подразделений и организаций, а также программно-целевого развития единого информационного пространства корпоративной проактивной киберсреды;
- сервисы выработки научно-обоснованных предложений для лиц, ответственных за реализацию политики ИБ, взаимосвязанных и согласованных мер киберзащиты организационного и технического характера;
- сервисы поддержки в актуальном состоянии информации об информационных ресурсах и ИИ корпоративных территориально-распределенных фрагментах КП;
- сервисы сбора, обработки и предоставления сведений подразделениям о выявлении в треке КП новых инцидентов по результатам мониторинга инцидентов в области ИТ и ИБ, реагирования на инциденты ИБ.

Описание сервисов КП предложено в [2] представлять с использованием известной в бизнес-телекоме процессной модели G^{eTOM} деятельности в функциональных областях eTOM (OPS, SIP, EM) в виде древовидного онтографа $G^{O}_{КП}$ путем прореживания $P^{eTOM}_{КП}$ и $P^{O}_{КП}$ тематического модельного слоя

eTOM на основе механизма методологии IDEF5, уточненного для онтологических исследований систем класса «киберполигон»,

$$G^{eTOM} \xrightarrow[P^{eTOM}_{\text{КП}}]{} G^{eTOM}_{\text{КП}} \xrightarrow[P^{O}_{\text{КП}}]{} G^{O}_{\text{КП}} = \begin{cases} G^{eTOM}_{OPS,\text{КП}} \xrightarrow[P^{O}_{\text{ТК,ТО,ТИ}}]{} G^{O}_{OPS,\text{КП}} \\ G^{eTOM}_{SIP,\text{КП}} \xrightarrow[P^{O}_{\text{ТК,ТО,ТИ}}]{} G^{O}_{SIP,\text{КП}} \\ G^{eTOM}_{EM,\text{КП}} \xrightarrow[P^{O}_{\text{ТК,ТО,ТИ}}]{} G^{O}_{EM,\text{КП}} \end{cases} . \quad (1)$$

Процессное описание сервисов треков КП опирается на графические модели в виде выборки упорядоченной взаимосвязи компонент онтографа $\mathrm{G^{eTOM}} =< \mathrm{N^{O}_{Tп}}, \mathrm{M^{O}_{Tп}}, \mathrm{V^{O}_{Tп}} >$ (концептов $\mathrm{N^{O}_{Tп}}$, отношений $\mathrm{M^{O}_{Tп}}$ и функций $\mathrm{V^{O}_{Tп}}$) с применением инструментальных CASE-средств моделирования бизнес-процессов. Пример процессного описания сервисов ТО ведомственного КП с использованием ERwin-средств представлен на Рис. 3.

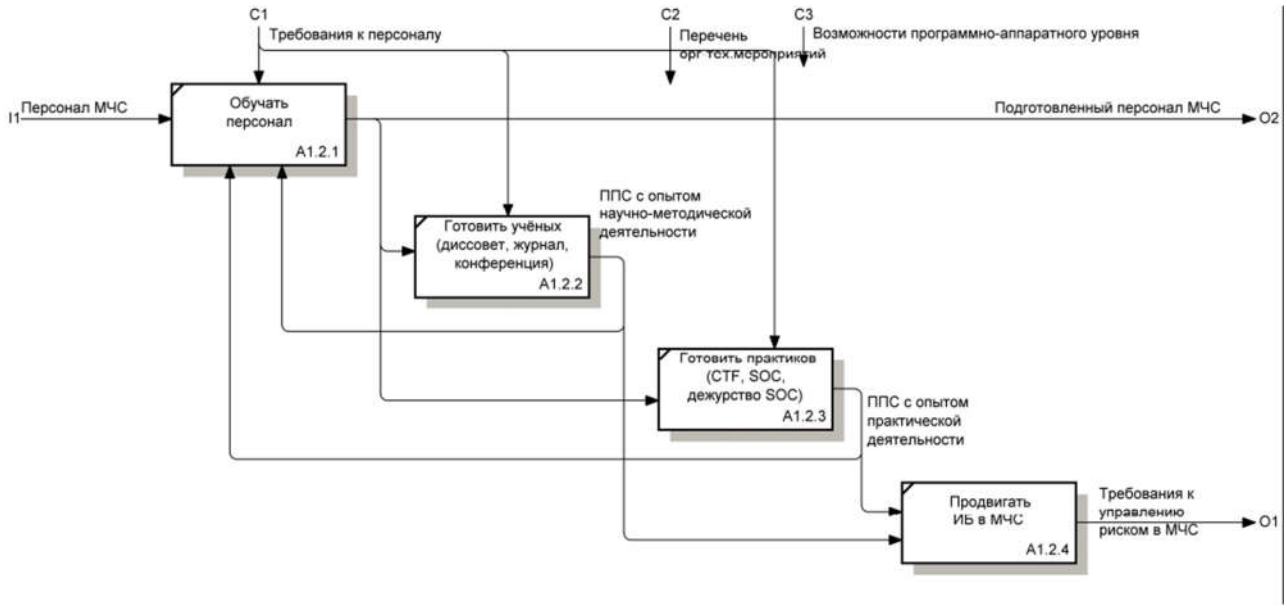

Рис. 3. Процессное описание сервиса образовательного трека ведомственного КП (фрагмент)

Такой подход к моделированию позволяет представить процессное описание сервисов КП в виде совокупности ориентированных ациклических графов на основе вершин онтографа $\mathrm{G^{O}_{КП}}$.

Синтез корпоративной системы повышения уровня осведомленности в области информационной безопасности

Результаты анализа типовых вариантов архитектур организации повышения уровня осведомленности персонала в области ИБ показывают, что применение сервисов внешнего или выделенного компонента (Рис. 4 а, 4 б) при изменении направлений потоков финансовых ресурсов несущественно отличаются в распределении традиционных функций и задач в структурных элементах корпоративной системы. Существенные изменения, а соответственно временные, ресурсные и финансовые затраты, будут при реализации архитектуры с интегрированным компонентом (Рис. 4 в).

Рис. 4. Архитектура систем повышения уровня осведомленности персонала в области информационной безопасности

Одной из принципиальных особенностей компонента является реализуемые им функции формирования и генерации тестирующих кибрвоздействий.

Задача синтеза такого варианта архитектуры с учетом введения в корпоративные подразделения распределенных элементов с потенциальными условно-реальными источниками киберугроз не является тривиальной и требует уточнения известной методологической базы [3, 4].

Предлагается синтез корпоративной системы повышения уровня осведомленности персонала проводить на основе процедур синтеза оргструктур по сервисным моделям онтографа $G^{O}_{КП}$с учетом ограничений в реализации функций кибервоздействий и возможности подразделений ИТ (ИБ) обеспечения в динамике их развития.

Перечень процедур характеризуется следующим.

Процедура формирования компонент модели организационной системы на основе архитектуры для сервисов интегрированного компонента (Рис. 4 в) выполняется с учетом существующих подразделений.

Процедура формирования сервисных процессных моделей заключается в формировании ориентированного ациклического (разомкнутого) гиперорграфа $G^{C}_{КП}$ в виде ∅ непустого конечного множества сгруппированных элементов $N^{O}_{Тп,КПi}$из подмножеств вершин $\left\{\left\{N^{O}_{Тп,ТК,КПi}\right\}\left\{N^{O}_{Тп,ТО,КПi}\right\}\left\{N^{O}_{Тп,ТИ,КПi}\right\}\right\}$, индексированных в соответствии с треками, и однонаправленных i,j - связей между ними $E^{C}_{КПij}$ как

$$G^{O}_{КП} \underset{P^{C}_{КП}}{\longrightarrow} G^{C}_{КП} = \begin{cases} < G^{O}_{OPS,КП}, G^{O}_{SIP,КП}, G^{O}_{EM,КП} > \underset{P^{C}_{ТК}}{\longrightarrow} G^{C}_{ТК,КП} \\ < G^{O}_{OPS,КП}, G^{O}_{SIP,КП}, G^{O}_{EM,КП} > \underset{P^{C}_{ТО}}{\longrightarrow} G^{C}_{ТО,КП} \\ < G^{O}_{OPS,КП}, G^{O}_{SIP,КП}, G^{O}_{EM,КП} > \underset{P^{C}_{ТИ}}{\longrightarrow} G^{C}_{ТИ,КП} \end{cases}. \quad (2)$$

Процедура декомпозиции гиперграфа $G^{C}_{КП}$ в матрицу $A_{N,N}$ достижимостей функций по каждому треку КП и оценки достаточности уровня декомпозиции проводится аналогично описанной в [3]:

для $\forall\ N^{O}_{Тп,КПi} \in \left\{\left\{N^{O}_{Тп,ТК,КПi}\right\}\left\{N^{O}_{Тп,ТО,КПi}\right\}\left\{N^{O}_{Тп,ТИ,КПi}\right\}\right\}$ (3)

$$N^{O}_{Тп,КПi}:\begin{cases}\{X_{ik}\}=\{I,C_i,R_i,K_i,t_i,D_i,L_i\},R_i=[0,1],K_i=[0,1]\\ a_{ij}=\{0.1\},N^{O}_{Тп,КПi}\to N^{O}_{Тп,КПj},i=1,N,j=1,N\\ \sum_j^N a_{ij}=1\,,i=1,N,j=1,N\end{cases}, \quad (4)$$

где X_{ik} - вектор параметров вершин; $I, C_i, R_i, K_i, t_i, D_i, L_i$ - параметры i-вершины (функции, затраты, компетентность, готовность, продолжительность принятия решений, деятельность, территориальность).

Процедура объединения матрицы $A_{N,N}$достижимости функций по всем сервисам КП осуществляется с применением матрицы смежности, в так называемую «процессно-организационную матрицу».

Процедура синтеза вариантов структуры системы повышения уровня осведомленности персонала является решением задачи поиска экстремального значения оценочной функции $F\{N^{O}_{Тп,КПi}, E^{C}_{КПij}\}$ из k-вариантов

$$F(X_{ik})\to \max(\min), \quad (5)$$

при ограничениях

$$\{f(X_{ik})\}><\{X_{jo}\} \quad (6)$$

по критерию готовности

для $\forall\, i=1,N: \sum_{j=1}^{N} a_{ij}^{r,\dots,m}=1$, (7)

$$K_г=\sum_i Q_i * \prod_{j=1} Kг_{ij}^{r,\dots,m}\left(a_{ij}^{r,\dots,m}\right)=max\ , \quad (8)$$

при $\sum_{i=1}^{n} Q_i=1$, (9)

$$R=\sum_i Q_i(\sum_{j=1}^{N} R_{ij}\, a_{ij}^{r,\dots,m}/\sum_{j=1}^{N} a_{ij}^{r,\dots,m})\geq R_o\ , \quad (10)$$

$$\sum_{r,\dots,m} C^{r,\dots,m}<C_o\ . \quad (11)$$

Процедура оценки и выбора рационального варианта структуры системы повышения уровня осведомленности персонала с учетом принятых ограничений и допущений проводится на основе критериев достижимости целей, оперативности (готовности организационных компонент и их взаимодействия), компетентности, внутренних киберрисков, стоимости. Важно отметить, что стоимость управления i-процессом C^i определяется стоимостью C_j управления i-функцией с учетом ее вклада в общий процесс (b_j^i) и стоимостью C_u^iэлемента i-процесса

$$C^i=\sum_{j=1}^{N} C_j b_j^i+C_u^i\ . \quad (12)$$

Исходя из значительности затрат на элемент процесса рассмотрим составляющую C_u^i более подробно.

Особенность технико-экономической оценки средств и оборудования киберполигона для подразделений ИТ(ИБ)-обеспечения заключается в определении, оценке и выборе варианта реализации, в частности, с привлечением специализированных компаний или собственных ресурсов [5]. По результатам технико-экономического анализа вариантов построения корпоративной системы типа «киберполигон» с применением метода анализа иерархий, выполненного коллективом ученых университета (Буйневич М.В., Шестаков А.В., Матвеев А.В.) в НИР «Вариант» в 2023 году, получены данные сравнительного анализа вариантов реализации КП (Табл. 1) и их обобщенная технико-экономическая оценка (Рис. 5).

Табл.1. Данные сравнительного анализа вариантов реализации киберполигона

Критерии	Варианты построения киберполигона						
	Коробоч-ное	Под ключ	Под ключ+	Заимст-вованное	Собствен-ное	Интегра-тора	Заказ-чика
	В-1	В-2	В-3	В-4	В-5	В-6	В-7
К-1 Масштаб	Small	Medium	Medium	Medium	Small	Large	Large
К-2 Функционал	Lim	Lim+	Lim+	Opt	Opt	Middle	Middle
К-3 Качество	Hight	Hight	Hight	Middle	Low	Middle	Middle-
К-4 Успех	≈ 100	> 90	> 90	50 - 60	30 - 40	> 90	70 - 90
К-5 Разработка	0	3-6	3-6	24 - 36	> 36	3 - 6	3 - 6
К-6 Внедрение	1 - 3	3 - 6	3 - 6	12-24	12-24	6 - 12	6 - 12
К-7 Персонал	Middle	Middle	Middle-	Middle	Hight	Middle	Hight
К-8 Затраты	Middle	Middle+	Middle++	Max	Max–	Min+	Min

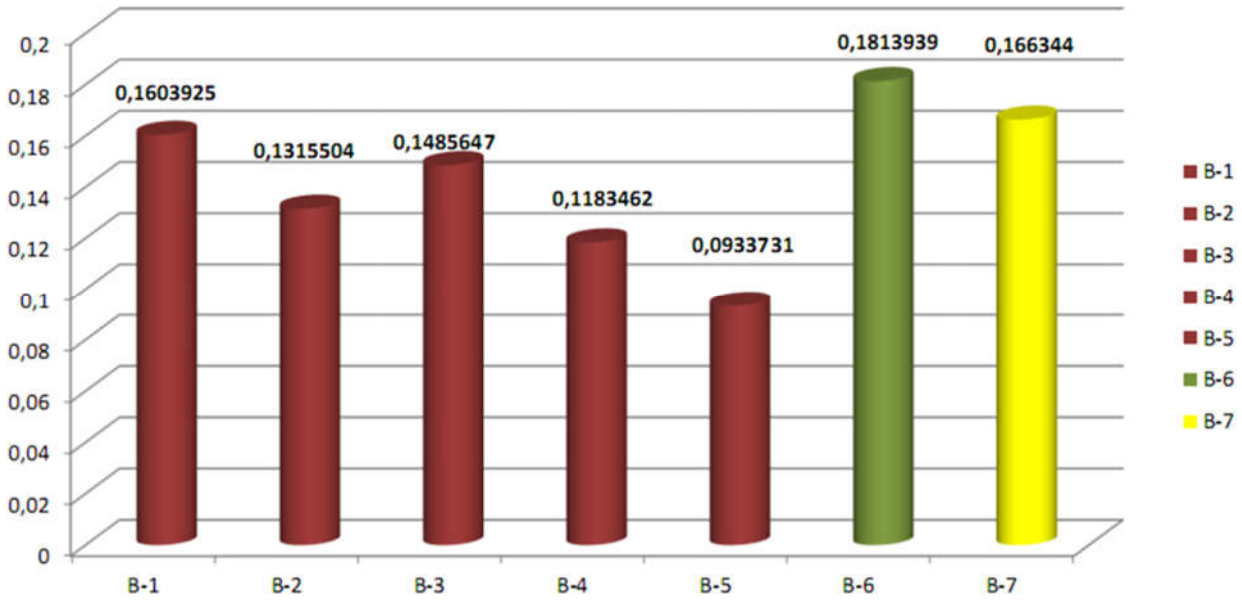

Рис. 5. Технико-экономическая оценка вариантов реализации киберполигона

Следует отметить, что решение «интегратора» наиболее рациональное для архитектуры сервисов интегрированного компонента, что показывают данные, представленные в Табл. 2.

Табл.2. Характеристики вариантов построения системы повышения осведомленности персонала

Перечень критериев	Архитектурный компонент системы			
	Внешний	Выделенный	Интегрированный	
Достижимость целей	Низкая	Средняя	Высокая	
Оперативность	Средняя	Средняя	Высокая	
Компетентность	Средняя	Высокая	Высокая	
Внутренние киберриски	Низкие	Средние	Низкие	Средние
Стоимость	Высокая	Средняя	Средняя+	

Процедура выработки рекомендаций по внедрению рационального варианта оргструктуры заключается в анализе результатов критериальной оценки и определение направлений по их снижению. С целью снижения внутренних киберрисков компонент КП, содержащий потенциальные

условно-реальные источники киберугроз должен быть выделенным в виде сегмента в корпоративной информационной инфраструктуре и иметь плановые конфигурации в виртуальной среде для реализации конкретных задач (сервисов) различных трактов.

Должны быть проведены и поддерживаться организационно-технические меры для предотвращения утечек и воздействий как результат функционирования развернутых условно-реальных источников киберугроз. Управление и распределение сервисов различных трактов выделенным сегментом должно осуществляться с применением специально разработанного программного конфигуратора с базой данных шаблонов виртуальных инфраструктур и данных для систем разграничения доступа корпоративной системы повышения уровня осведомленности персонала в области информационной безопасности.

Заключение

Комплексное решение задач повышения компетенций персонала, получения ими новых знаний, умений и навыков, а также задач расширения возможностей механизмов защиты информации (информационных ресурсов) и поддержки принятия решений систем обеспечения информационной безопасности структурных подразделений и корпоративной системы в целом, может быть обеспечено за счет внедрения перспективной образовательной технологии класса «киберполигон» в существующую информационную и организационную корпоративную инфраструктуру. Методологический подход к формированию рациональной корпоративной организационной системы на основе предложенных процедур позволит обеспечить устойчивое функционирование, эксплуатацию и развитие ключевых элементов (киберполигона) в условиях развития как киберугроз, методов атак, так и способов, и средств защиты информации.

Список источников

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

2. 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

3. Эффективное управление организационными и производственными структурами: монография / О.В. Логиновский, А.В Голлай, О.И. Дранко [и др.]; под ред. О.В. Логиновского. Москва: ИНФРА-М, 2020. 450 с.

4. Ильичев А.В., Ильичев В.М. Алгоритм синтеза организационной структуры управления по сигнальным графам моделей бизнес-процессов // Вестник Волжского университета им. В.Н. Татищева. 2010. № 20. С.180-186.

5. 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. EDN HSAZAO.

References

1. Buinevich M.V., Matveev A.V., Smirnov A.S. Current problems of training specialists in the field of information security of the Ministry of Emergency Situations of Russia and constructive approaches to their solution // Scientific-analyte. Journal. "Bulletin of St. Petersburg State University of the Ministry of Emergency Situations of Russia". 2023. No. 1. pp. 121-137. EDN OGPXZX.

2. Sineshchuk M.Yu., Shestakov A.V., Gavkalyuk B.V. Infological model and criteria for the quality of solutions for the construction of departmental organizational and technical systems of the class «cyberpolygon» // Scientific-analyte. Journal. "Bulletin of St. Petersburg State University of the Ministry of Emergency Situations of Russia". 2023. No. 1. pp. 121-137. EDN MYIAHH

3. Effective management of organizational and industrial structures: monograph / O.V. Loginovsky, A.V. Gollai, O.I. Dranko [et al.]; edited by O.V. Loginovsky. Moscow : INFRA-M, 2020. 450p.

4. Ilyichev A.V., Ilyichev V.M. Algorithm of synthesis of the organizational structure of management by signal graphs of business process models // Bulletin of the V.N. Tatishchev Volga State University. 2010. No. 20. pp.180-186.

5. Matveev A.V., Sineshchuk M.Yu., Shestakov A.V., Gavkalyuk B.V. Methodology for technical and economic assessment of options for constructing an organizational and technical system of the “cyber range” class // Engineering Bulletin of the Don. 2023. No. 6(102). pp. 187-200.

Статья поступила в редакция 23.01.2024; одобрена после рецензирования 01.03.2024; принята к публикации 21.03.2024.

The article was submitted 23.01.2024, approved after reviewing 01.03.2024, accepted for publication 21.03.2024.