ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.094

DOI: 10.21822/2073-6185-2024-51-2-83-90 Оригинальная статья / Original article

Применение методов динамического моделирования для создания адаптивной системы подготовки специалистов, отвечающей современным запросам в информационной сфере

А.М. Конаков, И.И. Лившиц
Национальный исследовательский университет ИТМО,
197101, г.Санкт-Петербург, Кронверкский пр., д. 49, Россия

Резюме. Цель. Целью исследования является анализ функциональных возможностей и особенностей динамического моделирования в рамках подготовки специалистов в области обеспечения информационной безопасности и противодействия различным угрозам в информационном пространстве с учетом временного фактора. **Метод.** Проведен анализ моделирования базового сценария возникновения инцидентов и угроз безопасности информации, который представляют собой исходные данные для формирования необходимого уровня и требований к подготовке специалистов информационной безопасности. **Результат.** Разработан и предложен новый подход к подготовке специалистов в области информационной безопасности с учетом современных запросов и требований. В предлагаемом подходе внедряется численный коэффициент, позволяющий определить область необходимых навыков и знаний для предотвращения и минимизации возможных инцидентов на промежутке времени. **Вывод.** Рассматриваемая область информационной безопасности, а именно подготовка квалифицированных специалистов, обладающих необходимым уровнем знаний и навыков, является актуальной с точки зрения развития информационно - технологического сектора и обеспечения защиты всех протекающих в нем процессов. Данная область требует дальнейшего внимания и внедрения новых подходов и методов подготовки в силу развития информационного общества и потребности в высококвалифицированных кадрах.

Ключевые слова: информационная безопасность, моделирование инцидентов, моделирование времени, динамические модели, графовые модели, анализ данных

Для цитирования: А.М. Конаков, И.И. Лившиц. Применение методов динамического моделирования для создания адаптивной системы подготовки специалистов, отвечающей современным запросам в информационной сфере. Вестник Дагестанского государственного технического университета. Технические науки. 2024; 51(2):83-90. DOI:10.21822/2073-6185-2024-51-2-83-90

The use of dynamic modeling methods to create an adaptive training system for specialists that meets modern demands in the information field

A.M. Konakov, I. I. Livshits
National Research University ITMO,
49 Kronverksky Ave., St. Petersburg 197101, Russia

Abstract. **Objective**. The purpose of the research is to analyze the functionality and features of dynamic modeling as part of training specialists in the field of information security and countering various threats in the information space, taking into account the time factor. **Method.** The analysis of modeling the basic scenario of incidents and threats to information security, which are the initial data for the formation of the necessary level and requirements for the training of information security specialists, is carried out **Result.** A new approach to training specialists in the field of information security has been developed and proposed, taking into account modern needs and requirements. The proposed approach introduces a numerical coeffi-

cient that allows us to determine the area of necessary skills and knowledge to prevent and minimize possible incidents over a period of time. **Conclusion.** The area of information security under consideration, namely the training of qualified specialists with the necessary level of knowledge and skills, is relevant from the point of view of the development of the information technology sector and ensuring the protection of all processes occurring in it. This area requires further attention and the introduction of new approaches and methods of training due to the development of the information society and the need for highly qualified personnel.

Keywords: information security, incident modeling, time modeling, dynamic models, graph models, data analysis

For citation: A.M. Konakov, I.I. Livshits. The use of dynamic modeling methods to create an adaptive training system for specialists that meets modern demands in the information field. Herald of Daghestan State Technical University. Technical Sciences. 2024; 51(2):83-90. DOI:10.21822/2073-6185-2024-51-2-83-90

Введение. Известно, что обеспечение информационной безопасности представляет собой все более актуальную проблему, которую нельзя обходить стороной. При всем этом, современные реалии развития и всеобъемлющего внедрения информационных технологий, а также сопутствующей технологической инфраструктуры представляют собой ключевой фактор необходимости реализации различных программ подготовки и соответствующего обучения специалистов, способных обеспечить безопасность всей рассматриваемой области и отдельных ее структурных элементов [1,2]. Также в стороне не остаются компании и организации, все больше понимающие необходимость защиты своих данных и информации от кибератак и взломов. В связи с этим, спрос на специалистов в области информационной безопасности растет, и все больше людей стремятся получить соответствующее образование, навыки и подготовку [3]. Подготовка таких специалистов как в общем, так и в индивидуальном (персональном) порядке, должна отвечать актуальным запросам информационной безопасности [4].

Постановка задачи. В работе предлагается подход, позволяющий в своей фундаментальной основе задействовать возможности динамического моделирования и графовых математических моделей для подготовки квалифицированных специалистов в области информационной безопасности [5]. Применение данных моделей позволит:

1. Осуществить более детализированный сбор и анализ данных для принятия соответствующих решений;
2. Обеспечить корректное прогнозирование необходимых навыков в определенный период времени;
3. Ориентироваться на реальные потребности и запросы в области обеспечения информационной безопасности;
4. Сформировать прочную структуру знаний и навыков (где есть понимание: для чего это нужно и зачем это нужно), которые необходимы для выполнения поставленных задач.

Методы исследования. Предлагаемый метод подготовки состоит из двух основных взаимосвязанных моделей и заключается в анализе исходных данных о защищаемых информационных системах, применяемых технологиях и методах защиты информации, с учетом рисков и угроз безопасности информации, и на основе полученной информации - интерпретации в наиболее оптимальный план подготовки специалистов с упором на критически важные модули обучения в соответствии с заданными требованиями.

Примером исходных данных для формирования может служить анализ реального сценария возникновения угроз безопасности информации, недопустимых событий и нанесения ущерба.

Результаты проведенного анализа 2-х сценариев реализации, представлены в табл. 1. и выполнены на основании «Методики оценки угроз безопасности информации» [6].

Таблица 1. Моделирование сценариев угроз безопасности, негативных событий и нанесения ущерба

Table 1. Modeling scenarios of security threats, negative events and damage

Наименование негативного событий Name of the Negative events	**Угроза безопасности Security Threat**	**Целевые информационные системы Targeted informational systems**	**Сценарии реализации Scripts Implementation**	**Критерии реализации Criteria implementation**
Хищение (кража) результатов интеллектуальной деятельности предприятия/ Theft (theft) of the results of intellectual activity of an enterprise	Нарушение работоспособности. Несанкционированный доступ к конфиденциальным данных и системе/ Malfunction Unauthorized access to confidential data and system	База данных и сопутствующие информационно - технологические ресурсы (хранения и обработка) для научно - исследовательских и опытно – конструкторских работ, а также работы с полученными результатами интеллектуальной деятельности/Database and related information and technological resources (storage and processing) for research and development work, as well as work with the results of intellectual activity obtained	Злоумышленник преодолел имеющиеся системы безопасности при использовании существующих уязвимостей и недостатков конфигурации системы защиты, с целью получения необходимых данных результатов интеллектуальной деятельности и дальнейшего хищения из системы хранения данных/ The attacker overcame the existing security systems by using existing vulnerabilities and deficiencies in the configuration of the security system	Получение доступа к Информационной системе с полным перечнем возможных привилегий. Получение доступа к прикладному ПО. Получение доступа к документам со значимой информацией и к целевой системе с определёнными привилегиями (правами доступа)/Obtaining access to the Information System with a full list of possible privileges; access to application software; access to documents with significant information; access to the target system with certain privilege
Хищение (кража) денежных средств и/ или других финансовых инструментов принадлежащих предприятию на правах собственности/ Theft (theft) of funds and/or other financial instruments owned by the enterprise	Нарушение работоспособности. Несанкционированный доступ к конфиденциальным данных и системе/ Malfunction Unauthorized access to confidential data and system.	База данных и сопутствующие информационно - технологические ресурсы для осуществления финансово - экономической и хозяйственной деятельности/ Database and accompanying information and technological resources for the implementation of financial, economic and business activities	Злоумышленник преодолел имеющиеся системы безопасности при использовании существующих уязвимостей и недостатков конфигурации системы защиты, с целью получения конфиденциальных данных финансово - экономической деятельности с последующим выводом денежных средств и/ или создания подложных документов для последующего обращения в финансовую организацию с последующим выводом денежных средств. The attacker overcame the existing security systems by using existing vulnerabilities and deficiencies in the configuration of the security system.	Получение доступа к Информационной системе с полным перечнем возможных привилегий. Получение доступа к прикладному ПО. Получение доступа к документам со значимой информацией.Получение доступа к целевой системе с определёнными привилегиями (правами доступа)/ Obtaining access to the Information System with a full list of possible privileges. Obtaining access to application software. Obtaining access to documents with significant information Gaining access to the target system with certain privileges (access rights)

Динамическое моделирование позволяет «спрогнозировать» на основе исходных данных наиболее критически уязвимые области информационного пространства, тем самым, выявить навыки и знания, необходимые специалистам в ходе их профессиональной деятельности в определенный диапазон времени [7, 8].

Так, на рис. 1 представлена кривая возможных инцидентов (X) и самих инцидентов (X_1, X_2, X_3) в зависимости от времени (t) и временных диапазонов (t_1, t_2, t_3 … t_n).

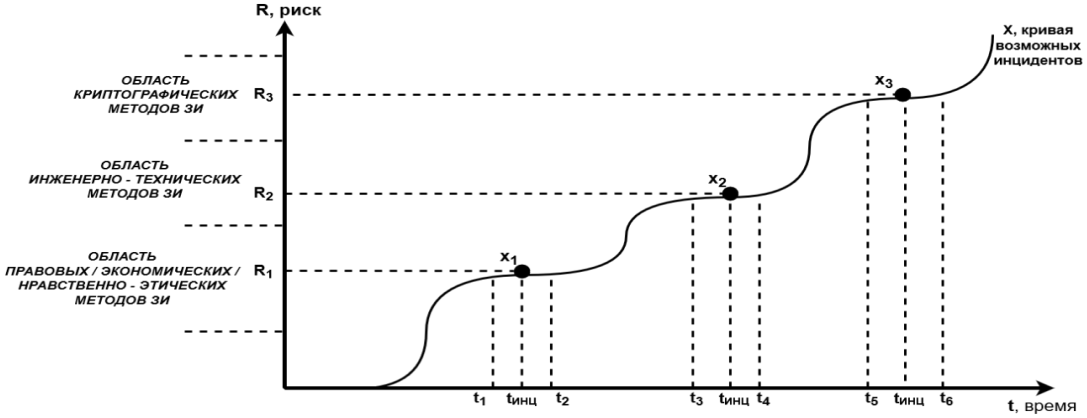

Рис. 1. Моделирование возможных инцидентов в зависимости от времени
Fig. 1. Modeling of possible incidents depending on time

Исходя из прогнозируемых инцидентов, диапазона времени их появления можно выявить прямую пропорциональность риска и наносимого ущерба системе с необходимым комплексом мероприятий по предотвращению возможного инцидента [9,10]. То есть, чем выше риск и объем наносимого ущерба системе, тем больше нужно консолидировать и задействовать ресурсов для их предотвращения и нейтрализации.

В свою очередь, использование графовых моделей при организации подготовки специалистов позволяет своими функциональными возможностями обеспечить плавный и сбалансированный переход от одного изучаемого модуля к другому за счет их связующих элементов [10]. Основанием такого использования графовых моделей является то, что при обеспечении информационной безопасности все внедряемые и используемые методы и средства защиты информации связаны между собой и представляют единый комплексный подход обеспечения безопасности информационно - технологической инфраструктуры [12]. То есть, графовые модели представляют собой наиболее удобный инструмент для визуального отображения и интерпретации, как это показано на рис. 2.

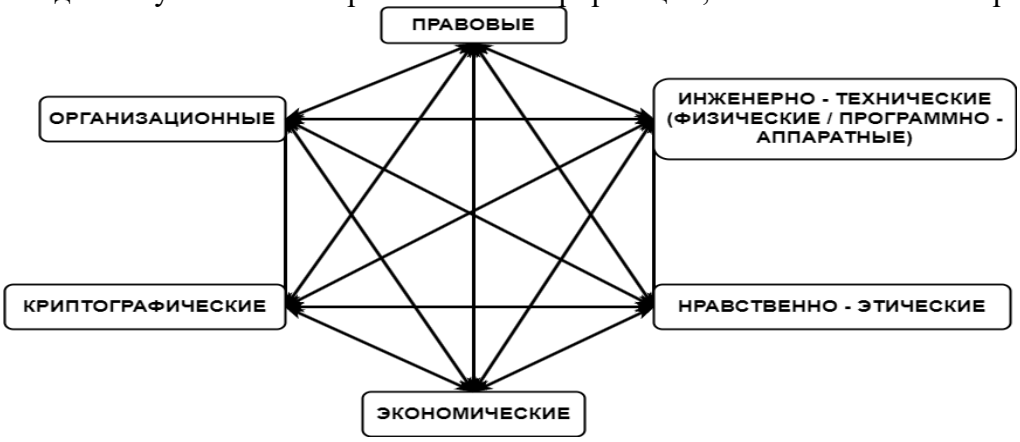

Рис. 2. Общая модель взаимосвязи методов защиты
Fig. 2. General model of the relationship between protection methods

Отличительной особенностью такого подхода является возможность «связки» между собой различных мер, методов и средств защиты информации, которые предстоит изучать, как это показано на рис. 3., где в каждом методе защиты информации есть множество структурных элементов, каждый из которых как отдельная единица, может быть взаимосвязан с элементами множеств других методов защиты. Реализация «связки» выполняется за счет того, что каждая реализуемая мера, средство или метод защиты и обеспечения безопасности имеют между собой сходные элементы внутри их фундаментальной структуры и/или при внедрении и эксплуатации на практике, не могут друг без друга эффективно противостоять угрозам [13].

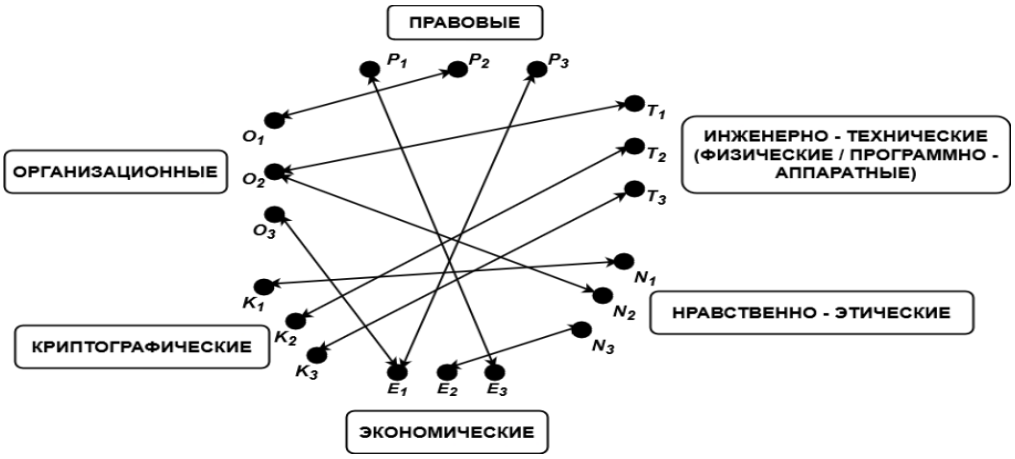

Рис. 3. Графовая модель взаимосвязи структурных элементов методов защиты информации
Fig. 3. Graph model of the relationship between the structural elements of information security methods

Именно благодаря такому способу можно осуществлять плавные переходы и консолидировать используемые ресурсы, а также в рамках подготовительных мероприятий наглядно показать, как можно наиболее эффективно достичь необходимый уровень безопасности выстраиваемой системы защиты информации.

Обсуждение результатов. В конечном итоге, на основе представленного подхода с использованием данных моделей, можно сформулировать и численно определить на основе вероятности возникновения ($P_{инц}$) инцидента и уровня риска (R), область необходимых знаний и методов защиты информации в конкретной ситуации (в том числе и диапазоне времени). Для этого вводится числовой коэффициент K, который определяется по следующей формуле:

$$K = P_{инц} * R$$

При этом должно соблюдаться условие: $R_{t(n)} < R_{t(n+1)}$

где: t(n) и t (n+1) – временные точки, определяющие приблизительный диапазон ($[t_n \ldots t_{n+1}]$) осуществления угрозы и возникновения инцидента.

В табл. 2 и табл. 3 представлены краткие характеристики и диапазоны принимаемых значений, вероятности возникновения инцидента $P_{инц}$, уровня риска R, коэффициента K. На основе полученных значений коэффициента, определяющего необходимый уровень знаний и навыков и уровня рисков, можно осуществить моделирование используемых мер и средств защиты в рамках подготовки специалистов.

Таблица 2. Описание принимаемых значений вероятности инцидента и риска
Table 2. Description of accepted values of incident probability and risk

№ п. п.	Вероятность инцидента $P_{инц}$ /Probability of incident P_inc	Оценка Риска R (принимаемые значения / краткая характеристика) Risk Assessment R (accepted values / brief description)	
1	$P_{инц} = [0 \ldots 1]$	1	Негативные последствия минимальны/ Negative consequences are minimal
2		2	Негативные последствия малозначительны/ Negative consequences are minor
3		3	Средний уровень негативных последствий/ Average level of negative consequences
4		4	Негативные последствия выше среднего/ Above average negative consequences
5		5	Негативные последствия значительные/ The negative consequences are significant
6		6	Негативные последствия критические Negative consequences are critical

Таблица 3. Характеристика соответствия значений коэффициента K методам защиты информации
Table 3. Characteristics of compliance of coefficient K values with information security methods

№ п.п.	Диапазон принимаемых значений вычисляемого коэффициента K Range of accepted values of the calculated coefficient K	Искомая область необходимых методов ЗИ Required area of required IR methods
1	[0…1]	Моральные / нравственно – этические/ Moral/ethical
2	(1…2]	Организационные/ Organizational
3	(2…3]	Правовые / Законодательные/ Legal/Legislative
4	(3…4]	Экономические/ Economic
5	(4…5]	Инженерно – технические/ Engineering - technical
6	(5…6]	Криптографические/ Cryptographic

При таком подходе будет проходить практическая подготовка и проверка знаний и умений на предмет анализа ситуации, прогнозирования дальнейших событий, аккумулирования используемых мер и средств защиты, которые нужны в определенный момент, их совместимости между собой и что самое главное – результативности противодействия угрозам и минимизации рисков, что напрямую связано с обеспечением безопасности и функционирования систем и защищаемых в них данных.

На рис. 4 представлено наглядное моделирование использования и совместимости мер из различных областей компетенций специалистов, необходимых для выполнения профессиональных задач.

На представленной схеме разными цветами обозначены результативный (зелёный) и нерезультативный (красный) варианты, в том числе, вариант (оранжевый) с промежуточной результативностью (где допущены ошибки при подборе, но при этом результативность может быть достигнута частично за счет некоторых мер из данного набора), а пунктирной линией между областями обозначены границы переходя от одного уровня знаний к другому (более высокому или низкому, в зависимости от текущей ситуации), основанные на оценке рисков.

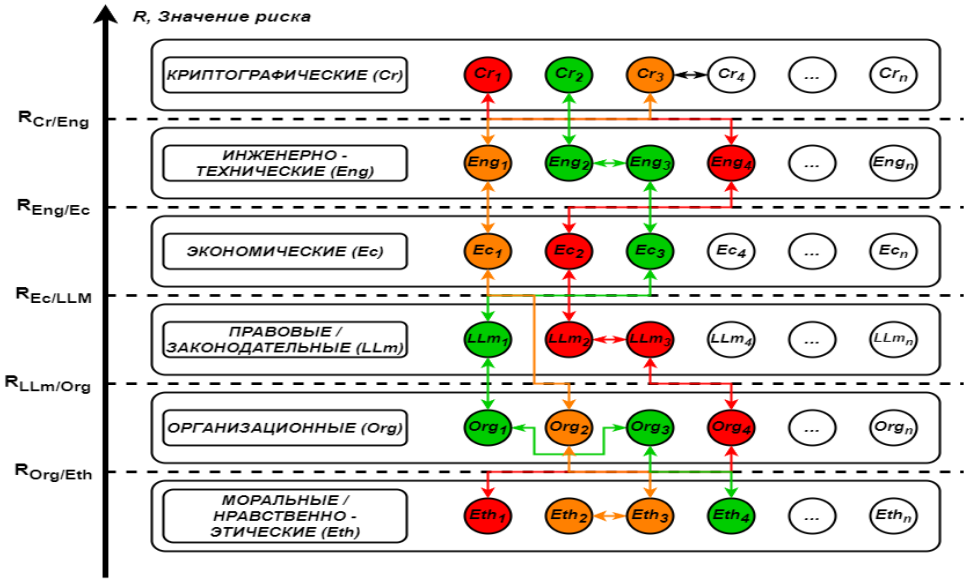

Рис. 4. Моделирование необходимого набора мер защиты в процессе подготовки
Fig. 4. Modeling the required set of protection measures during the preparation process

Такая визуализация и использование всех предложенных моделей позволяет оценить и проверить возможности специалистов, определить их профессиональный уровень, выявить недостатки в подготовке, а также наглядно продемонстрировать, как и за счет чего можно целей обеспечения информационной безопасности.

Вывод. Предложенный подход к подготовке специалистов в области информационной безопасности с использованием динамического моделирования представляет собой эффективный и инновационный метод с учётом современных реалий и требований.

Реализация методов моделирования при подготовке специалистов позволяет получать знания и навыки на реальных сценариях и ситуациях в гибком формате, что обеспечивает более глубокое и детальное освоение и понимание принципов информационной безопасности [14].

Данный подход способствует формированию компетентных специалистов, способных принимать решения в различных ситуациях, а также эффективно и адекватно реагировать на существующие риски и угрозы информационного пространства [15] за счет более удобной и практико – ориентированной (в основном, за счет графического моделирования и интерпретации) визуализации рисков в сочетании с требуемыми компетенциями в диапазонах времени.

Внедрение динамического моделирования в образовательно - подготовительный процесс позволяет создать адаптивную систему подготовки, отвечающую современным запросам в информационной сфере.

Библиографический список:

1. Магомедалиева М.Р., Халиев М.С.У. Обучение студентов различным способам защиты информации от компьютерной преступности //Профессионально - педагогическое образование: состояние и перспективы. – 2020. – С. 178-183.;
2. Шеер Е.Е. Актуальность вопроса подготовки квалифицированных специалистов в области информационной безопасности //Скиф. Вопросы студенческой науки. – 2021. – №. 1 (53). – С. 7-12.;
3. Братусин А.Р., Скобликов Р.В., Кашин О.В. О необходимости подготовки на базе вузов МВД и силовых ведомств РФ специалистов в области информационной безопасности //Проблемы современного педагогического образования. – 2019. – №. 63-4. – С. 27-31.;
4. Семенова З.В., Абросимова М.Г. Персонификация подготовки специалиста в области информационной безопасности //Актуальные проблемы обучения математике и информатике в школе и вузе. – 2021. – С. 432-443.;
5. Малюк А.А., Малюк З.П. Актуальные вопросы создания системы массового обучения культуре информационной безопасности //Безопасность информационных технологий. – 2021. – Т. 28. – №. 4. – С. 6-21.;
6. Методический документ «Методика оценки угроз безопасности информации» (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.);
7. Вострецова Е.В. Основы информационной безопасности: учебное пособие для студентов вузов / Е.В. Вострецова. — Екатеринбург: Изд-во Урал. ун-та, 2019. — 204 с.;
8. Батаргалиев А.А., Климентьев К.Е., Соловьева В.И. Научные и технические аспекты организации обучения вопросам защиты информации. – 2021. - С. 146-149.;
9. Александр Л., Горбылева Е.Л. Линейная динамическая модель угроз безопасности информации //Безопасность информационных технологий. – 2018. – Т. 25. – №. 3. – С. 53-66.;
10. Минаев В.А. и др. Системно-динамическое моделирование сетевых информационных операций //Инженерные технологии и системы. – 2019. – Т. 29. – №. 1. – С. 20-39.;
11. Щеглов А.Ю., Щеглов К.А. Математические модели и методы формального проектирования систем защиты информационных систем. Учебное пособие.– СПб: Университет ИТМО, 2015 – 93с.;
12. Ланкин О.В., Малышев С.А., Демченков А.В. О преимуществах графового представления функциональных моделей угроз информационной безопасности //Техника и безопасность объектов уголовно-исполнительной системы. – 2013. – С. 166-168.;
13. Гатчин Ю.А., Сухостат В.В., Куракин А.С., Донецкая Ю.В. Теория информационной безопасности и методология защиты информации – 2-е изд., испр. и доп. – СПб: Университет ИТМО, 2018. – 100 с.;
14. Кузнецова В.Ю. Аспекты оценки эффективности подготовки специалистов в области информационной безопасности //Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции. – 2019. – Т. 3.;
15. Попова Н.Ю., Тургенев В.А., Уральсков В.А. Особенности защиты информации при обучении специалистов на учебно-тренировочных средствах сложных технических систем //Вестник НИЦ ВА РВСН. – 2021. – №. 2. – С. 140-145.

References:

1. Magomedalieva M.R., Khaliev M.S.U. Teaching students various methods of protecting information from computer crime. *Professional pedagogical education: status and prospects*. 2020; 178-183. (In Russ)

2. Sheer E.E. Relevance of the issue of training qualified specialists in the field of information security. *Skif. Questions of student science*. 2021;1 (53):7-12. (In Russ)
3. Bratusin A.R., Skoblikov R.V., Kashin O.V. On the need to train specialists in the field of information security at universities of the Ministry of Internal Affairs and law enforcement agencies of the Russian Federation. *Problems of modern pedagogical education*. 2019;63(4):27-31. (In Russ)
4. Semenova Z.V., Abrosimova M.G. Personification of training a specialist in the field of information security. *Current problems of teaching mathematics and computer science at school and university*. 2021; 432-443.; (In Russ)
5. Malyuk A.A., Malyuk Z.P. Current issues of creating a system of mass training in the culture of information security. *Security of information technologies*. 2021; 28(4): 6-21. (In Russ)
6. Methodological document «Methodology for assessing information security threats» (approved by the Federal Service for Technical and Export Control on February 5, 2021); (In Russ)
7. Vostretsova E.V. Fundamentals of information security: a textbook for university students / E.V. Vostretsova. - Ekaterinburg: Ural Publishing House. Univ., 2019; 204. (In Russ)
8. Batargaliev A.A., Klimentyev K.E., Solovyova V.I. Scientific and technical aspects of organizing training in information security issues. 2021; 146-149. (In Russ)
9. Alexander L., Gorbyleva E.L. Linear dynamic model of threats to information security. *Information Technology Security*. 2018; 25(3):53-66. (In Russ)
10. Minaev V.A. et al. System-dynamic modeling of network information operations. *Engineering technologies and systems.* 2019; 29(1): 20-39(In Russ)
11. Shcheglov A.Yu., Shcheglov K.A. Mathematical models and methods for formal design of information systems security systems. Textbook. – St. Petersburg: ITMO University, 2015;93. (In Russ)
12. Lankin O.V., Malyshev S.A., Demchenkov A.V. On the advantages of graph representation of functional models of threats to information security. *Technology and security of objects of the penal system*. 2013; 166-168 (In Russ)
13. Gatchin Yu.A., Sukhostat V.V., Kurakin A.S., Donetskaya Yu.V. Theory of information security and methodology of information protection – 2nd ed., rev. and additional – St. Petersburg: ITMO University, 2018; 100. (In Russ)
14. Kuznetsova V.Yu. Aspects of assessing the effectiveness of training specialists in the field of information security. *Security Information Technologies. Collection of proceedings of the Tenth International Scientific and Technical Conference*. 2019;3. (In Russ)
15. Features of information protection when training specialists on training facilities for complex technical systems. *Bulletin of the Scientific Research Center of the Strategic Missile Forces of the Strategic Missile Forces*. 2021; 2: 140-145. (In Russ)

Сведения об авторах:
Конаков Александр Михайлович, магистрант, helium1937@yandex.ru.
Лившиц Илья Иосифович, доктор технических наук, профессор практики, Livshitz.i@yandex.ru
Information about authors:
Alexander M. Konakov, Master's student, helium1937@yandex.ru
Ilya I. Livshits, Dr. Sci.(Eng.), Prof. of Practice; Livshitz.i@yandex.ru
Конфликт интересов/Conflict of interest.
Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.
Поступила в редакцию/ Received 20.03.2024.
Одобрена после рецензирования/ Reviced 19.04.2024.
Принята в печать/ Accepted for publication 19.04.2024.