УДК 004.056.53 **DOI: 10.18413/2518-1092-2024-9-4-0-4**

Прокушев Я.Е.[1]
Пономаренко С.В.[2]
Белов А.С.[3]
Максимов Р.Р.[2]

ОПТИМИЗАЦИЯ ОБЪЕМА ТЕХНИЧЕСКИХ СРЕДСТВ МАШИННОГО ОБУЧЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ КЛЮЧЕВЫХ СИСТЕМ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

[1] Российский экономический университет имени Г.В. Плеханова,
Стремянный переулок, 36, г. Москва, 115054, Россия
[2] Белгородский университет кооперации, экономики и права,
ул. Садовая, 116а, г. Белгород, 308023, Россия
[3] Белгородский государственный национальный исследовательский университет,
ул. Победы, 85, г. Белгород, 308015, Россия

e-mail: prokye@list.ru, kaf-otzi-spec@bukep.ru, belovalex20122012@gmail.com, maksimov.riyan@mail.ru

Аннотация
Целью данной статьи является рассмотрение информационной деятельности систем защиты информации информационных инфраструктур органов государственного управления, обрабатывающих персональные данные с целью определения основных подходов к оптимизации объема технических средств системы защиты информации информационных инфраструктур с использованием средств машинного обучения, так как в рамках традиционного подхода защита информации ориентирована на преимущественно эвристические методы и использование интуитивных оценок изменения характеристик информационных процессов в результате проведения мероприятий по технической защите.
На основе анализа организации защиты информации заданного уровня (класса) защищенности инфосистемы органа государственного управления автор обосновывает комплексное использование машинного обучения системы защиты информации с целью оптимального использования функционального объема технических средств, выделяемых на обеспечение заданного уровня (класса) защищенности системы защиты информации органа государственного управления, обрабатывающего персональные данные.
В статье предложен ряд новых подходов оптимизации объема технических средств машинного обучения субъекта информационной инфраструктуры, обрабатывающего персональные данные.
Рассмотренные результаты позволили сформулировать задачу моделирования и оптимизации объема технических средств машинного обучения системы защиты информации для информационной деятельности органа государственного управления в условиях противодействия утечке информации по техническим каналам.
Ключевые слова: система защиты информации; оптимизация объема технических средств; машинное обучение; ключевые системы информационной инфраструктуры; условия обеспечения требуемого уровня (класса) защиты; алгоритмы имитационного моделирования информационных процедур и процедур технической защиты информации
Для цитирования: Прокушев Я.Е., Пономаренко С.В., Белов А.С., Максимов Р.Р. Оптимизация объема технических средств машинного обучения системы защиты информации ключевых систем информационной инфраструктуры // Научный результат. Информационные технологии. – Т.9, №4, 2024. – С. 36-43. DOI: 10.18413/2518-1092-2024-9-4-0-4

Prokushev Ya.E.[1]
Ponomarenko S.V.[2]
Belov A.S.[3]
Maksimov R.R.[2]

OPTIMIZATION OF THE VOLUME OF TECHNICAL MEANS OF MACHINE LEARNING OF THE INFORMATION PROTECTION SYSTEM OF KEY SYSTEMS OF INFORMATION INFRASTRUCTURE

[1] Plekhanov Russian University of Economics,
36 Stremyanny Lane, Moscow, 115054, Russia
[2] Belgorod University of Cooperation, Economics and Law,
116a Sadovaya St., Belgorod, 308023, Russia
[3] Belgorod State National Research University,
85 Pobedy St., Belgorod, 308015, Russia

e-mail: prokye@list.ru, kaf-otzi-spec@bukep.ru, belovalex20122012@gmail.com, maksimov.riyan@mail.ru

Abstract
The purpose of this article is to consider the information activities of information security systems of information infrastructures of government agencies processing personal data in order to determine the main approaches to optimizing the volume of technical means of the information security system of information infrastructures using machine learning tools, since within the framework of the traditional approach, information protection is focused mainly on heuristic methods and the use of intuitive assessments of changes in the characteristics of information processes as a result of technical protection measures.
Based on the analysis of the organization of information protection of a given level (class) of security of the information system of a government agency, the author substantiates the integrated use of machine learning of the information security system in order to optimally use the functional volume of technical means allocated to ensure a given level (class) of security of the information security system of a government agency processing personal data.
The article proposes a number of new approaches to optimizing the volume of technical means of machine learning of an information infrastructure entity processing personal data.
The considered results made it possible to formulate the problem of modeling and optimizing the volume of technical means of machine learning of the information security system for the information activities of a government agency in the context of counteracting information leakage through technical channels.
Keywords: information security system; optimization of the volume of technical means; machine learning; key information infrastructure systems; conditions for ensuring the required level (class) of protection; algorithms for simulation modeling of information procedures and procedures for technical protection of information
For citation: Prokushev Ya.E., Ponomarenko S.V., Belov A.S., Maksimov R.R. Optimization of the volume of technical means of machine learning of the information protection system of key systems of information infrastructure // Research result. Information technologies. – T.9, №4, 2024. – P. 36-43. DOI: 10.18413/2518-1092-2024-9-4-0-4

ВВЕДЕНИЕ

В последние десятилетия нейронные сети стали очень популярными благодаря доступности высокопроизводительных и недорогих компьютеров. Развитие вычислительной мощности позволило воплотить идеи изучения искусственного интеллекта, высказанные еще в 80-90-е годы. В середине 2000-х нейросетевое моделирование претерпело революцию с появлением алгоритмов глубокого обучения под руководством Джеффри Хинтона. Сегодня нейронные сети стали неотъемлемой частью нашей жизни, мы каждый день пользуемся ими, не задумываясь об этом, например, в распознавании речи, изображений, поиске информации в Интернете и построении систем защиты ключевых систем информационной безопасности (далее КСИИ) органов государственного управления (далее ГУ). [6]

1. Особенности информационной деятельности информационной системы защиты информации органов ГУ с использованием машинного обучения

Популярность специалистов в области машинного обучения системы защиты информации КСИИ и Data science органов ГУ на рынке труда растет, но нейросетевой подход пока не так широко используется в построении системы защиты КСИИ из-за неопределенности в обучении системы безопасности и сложности интерпретации результатов защищенности КСИИ при различных уровнях защищенности. Одной из причин этого может быть недостаток знаний в нейросетевом моделировании объемов необходимого задействованного оборудования системы защиты КСИИ и времени его использования для получения необходимого уровня защищенности. Существует различия в применении математических методов машинного обучения в построении системы защиты КСИИ органов ГУ: отечественные специалисты в области защиты информации чаще используют анализ различий в моделировании защищенности КСИИ органов ГУ в зависимости от объемов необходимого задействованного оборудования системы защиты КСИИ и заданного уровня защищенности КСИИ, в то время как зарубежные специалисты машинного обучения систем защиты предпочитают структурное моделирование структуры информационной системы, регрессионный анализ и метаанализ угроз информационной безопасности.

Российские специалисты в области машинного обучения систем защиты системы КСИИ обычно используют классические статистические методы машинного обучения в своих исследованиях необходимого уровня защищенности КСИИ органов ГУ, в то время как зарубежные ученые предпочитают новые и быстро развивающиеся методы определения необходимых объемов (время работы системы защиты, оптимизации структуры системы защиты в зависимости от выполняемых временных задач методом машинного обучения). Использование искусственных нейронных сетей в построении системы защиты информации КСИИ не так распространено, но все же некоторые исследования в этой области проводятся. Например, нейросетевое моделирование системы защиты КСИИ позволяет преодолеть ограничения классических статистических методов, такие как соотношение объема выборки и изучаемых параметров уровня защищенности, требование линейной зависимости и другие.

В современном мире информационная безопасность становится все более важной как для частных компаний, так и для государственных учреждений. В этом контексте нейронные сети, с их способностью к адаптации систем защиты КСИИ и обучению на больших объемах данных, играют важную роль в защите информации органов ГУ. Однако, помимо технических аспектов, эффективное обеспечение информационной безопасности КСИИ включает также психологические аспекты сотрудников служб защиты информации, особенно когда речь идет о поведении сотрудников внутри органа ГУ.

Нередко угрозы информационной безопасности КСИИ возникают изнутри органа ГУ, в частности из-за небрежного отношения сотрудников к конфиденциальной информации. Для более эффективного противодействия внутренним угрозам КСИИ, необходимо применять комплексный подход, включающий как машинное обучение технических средств защиты КСИИ, так и психологический анализ сотрудников органов ГУ.

Нейронные сети могут быть использованы для анализа обширных объемов данных органов ГУ, выявления аномалий и обучения моделей КСИИ, способных предсказывать потенциальные угрозы информационной безопасности. Эти технологии позволяют автоматизировать процессы мониторинга системы защиты и реагирования на инциденты, улучшая эффективность системы защиты КСИИ органа ГУ.

Преимущества использования нейросетей:

1. Глубокий анализ: нейронные сети органов ГУ эксплуатирующих систему защиты КСИИ могут обрабатывать большие объемы данных и выявлять скрытые шаблоны в поведении сотрудников и задействованного оборудования системы защиты информации.

2. Идентификация аномалий: способность нейросетей распознавать аномалии в поведении сотрудников органов ГУ эксплуатирующих систему защиты КСИИ может помочь в автоматизированном выявлении возникающих потенциальных угроз при заданном уровня защищенности (классе) СЗИ.

3. Автоматизация процесса: анализ угроз безопасности инфосистемы КСИИ (банк угроз информационной безопасности ФСТЭК РФ) с помощью нейросетей может быть автоматизирован, что снижает нагрузку на обслуживающий персонал инфосистемы и увеличивает эффективность задействованного оборудования СЗИ для обеспечения требуемого уровня (класса) защищенности КСИИ.

Для удовлетворения потребности защиты информации в машинном обучении инфраструктуры КСИИ необходимо выделить необходимый уровень (класс) защищенности инфосистемы и осуществить действия по оптимизации оптимального объема системы защиты информации КСИИ (при заданном уровне защищенности (классе)) на основании руководящих документов ФСТЭК РФ, направленных на обеспечение заданного состояние уровня (класса) защищенности КСИИ при оптимальном объеме задействованных средств для машинного обучения. Информативным признаком субъектно-объектных взаимодействий при реализации заданного уровне защищенности (классе) инфосистемы КСИИ является оптимизация инфосистемы защиты информации КСИИ на воздействие средств машинного обучения, реализующая требования руководящих документов ФСТЭК РФ по обеспечению требуемого уровня (класса) защищенности инфосистемы защиты КСИИ от оптимального объема. Средств машинного обучения. Результативность – это заданная защищенность системы от планируемых действий машинного обучения по оптимизации объема технических средств защиты информации инфосистемы КСИИ со свойствами оптимизации, скорости выявления угроз и сложности выполнения мероприятий защиты.

Для организации защиты информации инфосистемы КСИИ периодичность и объем процедур контроля должна соответствовать уровню угрозы утечки персональных данных при заданном уровне (классе) защищенности. Это позволяет повысить как эффективность мероприятий машинного обучения системы защиты информации информационных инфраструктур КСИИ по защите персональных данных, так и эффективность реализации отдельных процедур противодействия утечке информации с использованием методов машинного обучения.

Такой подход привел к необходимости решения ряда задач машинного обучения СЗИ КСИИ, связанных с оптимизацией используемых в процессе информационной деятельности технических и программных средств СЗИ КСИИ используемых из общего объема информационных (технических) ресурсов и разработки комплекса методик по их выявлению и использованию при заданном уровне защищенности (классе) инфосистемы КСИИ с использованием программных и технических средств машинного обучения. [6-12]

2. Использование аппарата математического моделирования для оптимизации системы защиты информации КСИИ

Оптимизация методов машинного обучения инфосистемы КСИИ заданного уровня (класса) защищенности подразумевает совершенствование разработанной ранее системы математического моделирования в подходах машинного обучения в решении задач оптимизации методов управления системой защиты инфосистемы КСИИ с целью математического представления оптимальных объемов необходимого задействованного технического оборудования для решения задач машинного обучения при заданных уровнях защищенности (классе) и оценки показателей задействованных оптимальных объемов технических средств машинного обучения, наиболее полно описывающих эти процессы со свойствами баланса эффективности оптимального объема технических средств.

Все это приводит к разработки математических и методических подходов разработки единой системы комплексного использования технических средств инфосистемы КСИИ, задействованных

для задач машинного обучения и рассмотрения методических подходов с целью минимизации использованных функциональных ресурсов и технических ресурсов из общего объема инфосистемы, задействованных для машинного обучения системы защиты информации (СЗИ) КСИИ, а также технических средств информатизации, задействованных на обеспечение управления СЗИ КСИИ, обрабатывающей персональные данные.

Для оценки результативности (обоснованности) математических и методических подходов разработки единой системы комплексного использования технических средств инфосистемы КСИИ в условиях управления формированием оптимальной системы машинного обучения для заданного уровня (класса) защищенности инфосистемы КСИИ, обрабатывающего персональные данные в работе необходимо использовать ряд показателей. К ним можно отнести:

– полноту реализации оптимальных информационных действий системы машинного обучения для управления формированием заданного уровня защищенности (класса) информационного ресурса инфосистемы СЗИ КСИИ, обрабатывающего персональные данные;

– защищенность (класс) информационной инфраструктуры КСИИ при машинном обучении при различных уровнях заданной защищенности (классе) информационной системы КСИИ, обрабатывающей персональные данные.

– качество реализации информационных процессов инфосистемы СЗИ КСИИ является показателем эффективности этих процессов с использованием требуемого оптимального объема технических средств для машинного обучения. В качестве данного показателя предлагается использовать вероятность того, что объем реализуемых процедур машинного обучения информационной деятельности инфосистемы КСИИ не меньше требуемого значения при заданном уровне защищенности (классе) СЗИ. [1-5]

3. Алгоритм вычисления требуемого объема реализации информационных процедур машинного обучения при заданном уровне защищенности КСИИ

Информационный процесс инфосистем КСИИ реализующих процедуры машинного обучения информационной деятельности системы защиты КСИИ считается выполненным в полном объеме, если объем процедур (при заданном уровне защищенности (классе) СЗИ) машинного обучения $O_{(n)}$ выполняемых мероприятий информационной деятельности не меньше требуемой величины $O_{(з)}$ при заданном уровне защищенности (классе) СЗИ), т.е. при выполнении неравенства:

$$O_{(n)} \geq O_{(з)} \quad (1)$$

Заданный объем $O_{(з)}$ оборудования системы защиты для машинного обучения информационной деятельности КСИИ не меньше требуемого значения при заданном уровне защищенности определяется нормативными и организационно-распорядительными документами ФСТЭК РФ, определяющими функционирование инфосистемы КСИИ в зависимости от заданного уровня защищенности (класса) СЗИ.

При таком подходе входящая в неравенство заданная величина $O_{(з)}$ определяемая руководящими документами ФСТЭК РФ будет являться случайной величиной зависящей от уровня защищенности (класса) СЗИ. Выполнение действий по оптимизации объема технических средств СЗИ КСИИ является прогнозируемым событием при машинном обучении СЗИ, определяемый требуемой вероятностью реализации процедур несанкционированного доступа (НСД) при заданном уровне защищенности инфосистемы СЗИ КСИИ в соответствии с руководящими документами ФСТЭК РФ:

$$E = P(O_{(n)} \geq O_{(з)}) \quad (2)$$

Одним из параметров заданной защищенности инфосистемы КСИИ от утечки по техническим каналам с использованием машинного обучения инфосистемы СЗИ КСИИ планируется использовать вероятность того, что оптимальный объем технических средств машинного обучения при заданном уровне защищенности (классе) СЗИ процедур НСД информации не меньше допустимого значения.

Мероприятия технической защиты информации (ТЗИ) с использованием средств машинного обучения СЗИ инфосистемы КСИИ в соответствии с их заданной руководящими документами ФСТЭК РФ структурой $F_{(n)}$ в составе действующей структуры $F_{(з)}$ мероприятий функционирования машинного обучения СЗИ считаются выполненными в полном объеме при заданном уровне защищенности уровне (классе) СЗИ КСИИ $F_{(сзи)}$, если их заданный объем $O_{(n)}$ процедур ТЗИ с использованием машинного обучения не меньше минимально необходимой величины инфосистемы КСИИ $O_{(з)}$ при оптимальном объеме технических средств задействованных для машинного обучения СЗИ КСИИ:

$$O_{(з)}(F_{(n)}, F_{(з)}, O_{(n)}(t), F_{(сзи)}) \geq O_{(n)}(U(t)) \quad (3)$$

Вероятностный характер условий информационной деятельности инфосистемы КСИИ при машинном обучении СЗИ КСИИ при заданном уровне (классе) защищенности, описываемых множеством $O_{(n)}$ при оптимальном объеме задействованных технических средств машинного обучения системы защиты КСИИ, и мероприятий защиты от НСД при заданном ФСТЭК РФ уровне защищенности (классе) инфосистемы СЗИ КСИИ, описываемых множеством $U(t)$, позволяет сделать заключение о том, что объем $O_{(n)}$ является расчетной величиной в зависимости от заданного уровня (класса) защищенности КСИИ на основании базовой модели угроз ФСТЭК РФ.

Минимально необходимый объем технических средств $O_{(n)}$ реализации процедур машинного обучения технической защиты информации в инфосистемы СЗИ КСИИ определяется характером угрозы утечки информации с использованием средств несанкционированного доступа к КСИИ, оптимальным объемом задействованных технических и программных средств используемых для машинного обучения СЗИ КСИИ при заданной защищенности (классе) с использованием базовой модели угроз ФСТЭК РФ.

В данном случае входящие в неравенство (4) величины являются случайными, поэтому его реализация является случайным событием, характеризуемым соответствующей вероятностью в зависимости от заданных ФСТЭК РФ величин уровня защищенности (классе) СЗИ:

$$S = P(O_{(n)} \geq O_{(з)}) \quad (4)$$

Это позволило решить задачу моделирования и оптимизации системы машинного обучения СЗИ инфосистемы КСИИ в условиях противодействия утечке информации с использованием технических и программных средств НСД. В методологическом плане такой подход формулируется как задача разработки моделей и алгоритмов оптимизации объема технических средств, задействованных для машинного обучения инфосистемы КСИИ в интересах обеспечения защиты от НСД в процессе ее эксплуатации.

Основными принципами решения оптимизации объема технических средств, задействованных для машинного обучения инфосистемы КСИИ, по моему мнению, являются:

– принцип согласованности информационной деятельности по реализации оптимизации объема технических средств, задействованных для машинного обучения инфосистемы КСИИ при заданном уровне (классе) защищенности;

– принцип резервируемости объема технических средств, задействованных для машинного обучения инфосистемы КСИИ;

– принцип одновременной реализации двух разнородных видов технических средств, задействованных для машинного обучения инфосистемы КСИИ в зависимости от уровня (класса) защищенности инфосистемы КСИИ;

– принцип баланса эффективности оптимального объема технических средств, задействованных для машинного обучения инфосистемы КСИИ.

ВЫВОДЫ И ЗАКЛЮЧЕНИЕ

Результаты формализации оптимального объема технических средств, задействованных для машинного обучения инфосистемы КСИИ в условиях обеспечения требуемого уровня (класса) защиты КСИИ от утечки по техническим каналам являются исходными данными для алгоритмов

имитационного моделирования информационных процедур и процедур технической защиты информации.

Список литературы

1. Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и защите информации».

2. Федеральный закон № 187-ФЗ от 27 июля 2017 года «О безопасности критической информационной инфраструктуры Российской Федерации».

3. Постановление правительства Российской Федерации от 08 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

4. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

5. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

6. Пономаренко С.В., Пономаренко С.А., Прокушев Я.Е. Информационная безопасность критических систем информационной инфраструктуры: монография. Белгород: БУКЭП, 2021. – 133 с.

7. Прокушев Я.Е., Пономаренко С.В., Пономаренко С.А. Моделирование процессов проектирования систем защиты информации в государственных информационных системах // Computational Nanotechnology. 2021. – Т. 8. – № 1. – С. 26–37.

8. Прокушев Я.Е., Пономаренко С.В., Шишов Н.В. Моделирование процессов проектирования систем защиты информации в критических информационных инфраструктурах // Computational Nanotechnology. 2022. – Т. 9. – № 2. – С. 45–55.

9. Бирюков М.В., Климова Н.А., Гостищева Т.В. Оценка затрат на проведение мероприятий по обеспечению информационной безопасности организаций потребкооперации // Экономика. Информатика. – 2020. – Т.47. – №1. – С. 101-109.

10. Бирюков М.В., Климова Н.А., Гостищева Т.В. О самообучающихся машинных системах в процессе авторизации пользователей банкоматов // Экономика. Информатика. – 2020. – Том 47. – №2. – С. 354-361.

11. Ломазов В.А., Пономарев Д.В., Пономаренко С.В. Эволюционный синтез иерархии оценочных показателей проекта в сфере информационной безопасности // Глобальный научный потенциал. – 2017. – № 11 (80). – С.82-85.

12. Пономаренко С.В., Бирюков М.В., Климова Н.А. Экономические перспективы использования технологии дистанционного банковского обслуживания // Вестник Белгородского университета кооперации, экономики и права. Белгород: Издательство БУКЭП. – Выпуск 1(68) – 2018. – С. 159-167.

13. Прокушев Я.Е., Пономаренко С.В. Сравнительный анализ средств программно-аппаратной защиты информации, применяемых в информационных системах персональных данных // Информация и безопасность. – 2012. – Т. 15. – № 1. – С. 31–36.

14. Прокушева А.П., Прокушев Я.Е. Моделирование и оптимизация выбора средств программно-аппаратной защиты информации с точки зрения экономической и технической целесообразности // Информация и безопасность. 2012. – Т. 15. – № 1. – С. 55–60.

15. Mattord H., Whitman M. Management of information security. 6th ed. Cengage Learning, 2019. – 752 p.

16. Rohit Tanwar. Information security and optimization. CRC Press, 2021. – 224 p.

17. Whitman M.E. et al. PRSCIiples of information security. 6th ed. Cengage Learning, 2017. – 656 p.

References

1. Federal Law No. 149-FZ of July 27, 2006 «On Information, Information Technologies and Information Protection».

2. Federal Law No. 187-FZ of July 27, 2006 «On the security of the critical information infrastructure of the Russian Federation».

3. Decree of the Government of the Russian Federation of February 08, 2018 No. 127 «On approval of the Rules for categorizing objects of critical information infrastructure of the Russian Federation and the list of indicators of criteria for the significance of objects of critical information infrastructure of the Russian Federation and their values».

4. Order No. 21 «On approval of the composition and content of organizational and technical measures to ensure the security of personal data during their processing in personal data information systems». Approved by FSTEC of Russia of 18.02.2013.

5. Order No. 239 «On approval of the Requirements for ensuring the security of significant objects of critical information infrastructure of the Russian Federation». Approved by FSTEC of Russia of 25.12.2017.

6. Ponomarenko S.V., Prokushev Ya.E., Ponomarenko S.A. Information security of critical information infrastructure systems. Monography. Belgorod: BUKEP, 2021. – 133 p.

7. Prokushev Ya.E., Ponomarenko S.V., Ponomarenko S.A. The modeling of information security system design processes in state information systems. Computational Nanotechnology. – 2021. – Vol. 8. – No. 1. – Pp. 26–37. (in Russian)

8. Prokushev Ya.E., Ponomarenko S.V., Shishov N.V. The modeling of processes of design of information protection systems in critical information infrastructures. Computational Nanotechnology. – 2022. – Vol. 9. – No. 2. – Pp. 45–55. (in Russian)

9. Biryukov M.V., Klimova N.A., Gostishcheva T.V. Cost estimate on implementation of measures, ensuring information security in consumer cooperation organizations // Economics. Information technologies. – 2020. – Vol. 47. – № 1. – P. 101-109.

10. Biryukov M.V., Klimova N.A., Gostishcheva T.V. About self-learning machine systems in the process of authorization of users of ATMs // Economics. Information technologies. – 2020. – Vol. 47. – № 2. – P. 354-361.

11. Lomazov V.A., Ponomarev D.V., Ponomarenko S.V. Evolutionary synthesis of the hierarchy of estimated indicators of the project in the field of information security // Global scientific potential. – 2017. – № 11 (80). – P.82-85.

12. Ponomarenko S.V., Biryukov M.V., Klimova N.A. Economic prospects for the use of remote banking technology // Bulletin of the Belgorod University of Cooperation, Economics and Law. Belgorod: BUKEP Publishing House. – Issue 1 (68) – 2018.

13. Prokushev Ya.E., Ponomarenko S.V. Comparative analysis of software and hardware protection of information used in information systems of personal data. Information and Security. – 2012. – Vol. 15. – №. 1. – Pp. 31–36. (in Russian)

14. Prokusheva A.P., Prokushev Ya.E. Modeling and optimization of the choice of software and hardware protection of information from the point of view of economic and technical expediency. Information and Security. 2012. – Vol. 15. – No. 1. – Pp. 55–60. (in Russian)

15. Mattord H., Whitman M. Management of information security. 6th ed. Cengage Learning, 2019. – 752 p.

16. Rohit Tanwar. Information security and optimization. CRC Press, 2021. – 224 p.

17. Whitman M.E. et al. PRSCIiples of information security. 6th ed. Cengage Learning, 2017. – 656 p.

Прокушев Ярослав Евгеньевич, кандидат экономических наук, доцент, доцент кафедры прикладной информатики и информационной безопасности
Пономаренко Сергей Владимирович, кандидат технических наук, доцент, профессор кафедры информационная безопасность
Белов Александр Сергеевич, кандидат технических наук, доцент, доцент кафедры автоматизированных систем и технологий
Максимов Риян Ренатович, аспирант кафедры информационная безопасность

Prokushev Yaroslav Evgenievich, Candidate of Economic Sciences, Associate Professor, Associate Professor, Department of Applied Informatics and Information Security
Ponomarenko Sergey Vladimirovich, Candidate of Technical Sciences, Associate Professor, Professor of the Department of Information Security
Belov Alexander Sergeevich, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Automated Systems and Technologies
Maksimov Riyan Renatovich, Graduate Student of the Information Security Department