DOI: 10.25198/1814-6457-249-49
УДК 378.147:004

Влацкая И.В.
Оренбургский государственный университет, г. Оренбург, Россия
E-mail: irina.vlatskaya@yandex.ru

ОТ МЕТОДОЛОГИИ КИБЕРИММУНИТЕТА ДО КОНСТРУКТИВНОЙ БЕЗОПАСНОСТИ ПРИ ПОДГОТОВКЕ ОБУЧАЮЩИХСЯ НА ИНФОРМАЦИОННЫХ НАПРАВЛЕНИЯХ СПЕЦИАЛИТЕТА И БАКАЛАВРИАТА

В условиях цифровизации и роста сложности информационных систем традиционные подходы к обеспечению информационной безопасности, основанные преимущественно на реактивных мерах защиты, демонстрируют ограниченную эффективность. Современные кибератаки характеризуются высокой степенью автоматизации, использованием интеллектуальных методов анализа и эксплуатации уязвимостей, а также ориентацией на архитектурные и логические дефекты информационных систем. Это обуславливает необходимость перехода от периметровых и надстроечных моделей защиты к архитектурно ориентированным подходам, предполагающим формирование защищённости на этапе проектирования информационных систем. В ходе проведённого исследования проанализирована методология кибериммунитета, разработанная специалистами Лаборатории Касперского, и её развитие в рамках концепции конструктивной безопасности. Архитектурные принципы минимизации доверия, изоляции компонентов и управления потоками информации, реализуемые в архитектурах MILS и FLASK внедрены в образовательный процесс Оренбургского государственного университета. Их эффективность выразилось в повышении качества обучаемости, улучшении уровня сформированности профессиональных компетенций обучающихся, а также в успешной апробации разработанных прикладных программных средств и методов анализа данных. Интеграция методологии кибериммунитета и конструктивной безопасности в подготовку обучающихся по информационным направлениям обеспечивает методологическую основу для формирования системного инженерного мышления. Освоение архитектурно ориентированных подходов к обеспечению безопасности способствует переходу от фрагментарного изучения отдельных средств защиты к целостному пониманию принципов построения устойчивых к угрозам информационных систем, что подтверждает целесообразность и результативность их использования в образовательном процессе подготовки специалистов и бакалавров в области информационных технологий и информационной безопасности.

Ключевые слова: информационные технологии, информационная безопасность, кибериммунитет, конструктивная безопасность, MILS, FLASK, архитектура Zero Trust.

Vlatskaya I.V.
Orenburg State University; Orenburg, Russia
E-mail: irina.vlatskaya@yandex.ru

FROM THE CYBER IMMUNITY METHODOLOGY TO CONSTRUCTIVE SECURITY IN THE EDUCATION OF SPECIALIST AND BACHELOR STUDENTS IN INFORMATION AND INFORMATION TECHNOLOGY PROGRAMS

In the context of digitalization and the increasing complexity of information systems, traditional approaches to information security, primarily based on reactive protective measures, demonstrate limited effectiveness. Modern cyberattacks are characterized by a high degree of automation, the use of intelligent methods for vulnerability analysis and exploitation, as well as a focus on architectural and logical flaws in information systems. In this regard, the need to transition from perimeter-based and add-on security models to architecture-oriented approaches becomes increasingly relevant.

This article examines the cyber immunity methodology proposed by Kaspersky Lab specialists as a modern paradigm for ensuring information security. It is shown that cyber immunity involves designing systems that are resilient to attacks by virtue of their architecture, rather than through the use of external security tools. Particular attention is paid to constructive security as a practical development of cyber immunity principles. The architectural concepts of MILS and FLASK are analyzed, along with their role in minimizing trust and controlling information flows.

The relationship between constructive security and contemporary international and Russian information security standards is also considered. The importance of studying these approaches in the educational process for training specialists and bachelor students enrolled in information and information technology programs is emphasized.

Keywords: information technologies, information security, cyber immunity, constructive security, MILS, FLASK, Zero Trust architecture.

Современные информационные системы характеризуются высокой степенью распределённости, интеграцией облачных технологий, киберфизических компонентов и интеллектуальных сервисов. Эти факторы существенно усложняют задачу обеспечения информационной безопасности и требуют от специалистов не только навыков эксплуатации защитных средств, но и способности проектировать системы, устойчивые к угрозам на архитектурном уровне [1].

В условиях усложнения киберугроз, включая атаки с применением искусственного интеллекта, традиционные реактивные подходы к безопасности демонстрируют ограниченную эффективность [2]. Это обстоятельство обуславливает необходимость пересмотра не только технических решений, но и подходов к подготовке специалистов в области информационных технологий и компьютерной безопасности.

Для таких образовательных программ, реализуемых в Оренбургском государственном университете, актуальной задачей становится формирование у студентов системного инженерного мышления, ориентированного на безопасность как неотъемлемое свойство проектируемых систем. В этом контексте методология кибериммунитета представляет собой не только современную научно-техническую концепцию, но и эффективную дидактическую основу для обучения будущих специалистов.

Включение принципов кибериммунитета в учебный процесс позволяет сместить акцент с изучения отдельных средств защиты на анализ архитектурных решений, моделей доверия и формальных политик безопасности, что соответствует современным требованиям к инженерному образованию в области информационной безопасности.

Исторически обучение информационной безопасности базировалось на периметровой модели защиты, в рамках которой внутренняя сеть рассматривалась как доверенная, а внешняя — как потенциально враждебная [2]. Данный подход нашёл отражение и в образовательных курсах, ориентированных преимущественно на администрирование межсетевых экранов, антивирусных средств и систем обнаружения вторжений.

Однако развитие распределённых систем, удалённого доступа и сервисно-ориентированных архитектур привело к размыванию границ периметра, что существенно снизило практическую применимость классических моделей [3]. В результате в образовательном процессе возник разрыв между изучаемыми концепциями и реальными архитектурными решениями, используемыми в современных информационных системах.

Переход к многоуровневым моделям защиты и концепции defense in depth частично расширил спектр рассматриваемых угроз, однако по-прежнему сохранял ориентацию на реактивные меры [4]. Для студентов это выражалось в фрагментарном восприятии безопасности как набора разрозненных инструментов, а не как системного свойства.

Методология кибериммунитета, напротив, позволяет выстроить обучение на основе архитектурного и проектного подхода, в рамках которого:

– безопасность рассматривается на этапе проектирования;

– анализируются модели доверия и взаимодействия компонентов;

– формируются навыки формализации требований безопасности.

С педагогической точки зрения кибериммунитет способствует развитию у студентов:

– инженерного мышления;

– способности анализировать архитектурные компромиссы;

– понимания взаимосвязи между функциональностью и безопасностью.

Таким образом, эволюция подходов к проектированию информационных систем и обеспечению их безопасности объективно требует трансформации образовательных программ, в которых методология кибериммунитета и концепция конструктивной безопасности выступают методологическим каркасом подготовки специалистов нового поколения.

Методология кибериммунитета была сформулирована специалистами Лаборатория Касперского как ответ на фундаментальные ограничения реактивных моделей информационной безопасности [6]. В отличие от периметровых и сигнатурных подходов, кибериммунитет исходит из предположения, что атака возможна всегда, а потому ключевой задачей является инженерное ограничение последствий компрометации.

В рамках данной методологии безопасность рассматривается как архитектурное свойство си-

стемы, формируемое на этапе проектирования, а не как совокупность внешних защитных средств.

Кибериммунитет базируется на наборе архитектурных принципов, направленных на снижение доверия и повышение предсказуемости поведения системы [6], [8].

Ключевыми принципами являются:

Минимизация доверия — ни один компонент не считается доверенным по умолчанию;

Изоляция — процессы и данные разделяются на независимые домены;

Формализуемость — правила взаимодействия компонентов описываются в виде политик безопасности;

Ограничение ущерба — компрометация одного компонента не должна приводить к отказу всей системы.

Эти принципы реализуются через строгую архитектурную декомпозицию и контроль взаимодействий, представленные на рисунке 1.

Архитектура MILS (Multiple Independent Levels of Security) представляет собой один из ключевых технологических механизмов реализации кибериммунитета [7]. В основе MILS лежит идея разделения системы на независимые домены безопасности с различными уровнями доверия. Архитектура MILS представлена на рисунке 2.

Каждый домен:

– выполняет строго определённые функции;

– не имеет прямого доступа к другим доменам;

– взаимодействует с ними исключительно через контролируемые интерфейсы.

Центральным элементом архитектуры MILS является минимальное ядро (separation kernel), отвечающее исключительно за:

– изоляцию;

– маршрутизацию сообщений;

– соблюдение политик безопасности.

Применение MILS позволяет существенно сократить доверенную вычислительную базу и повысить формальную проверяемость системы [8].

Еще одним механизмом кибериммунитета является архитектура FLASK (Flux Advanced Security Kernel) ориентирована на контроль информационных потоков внутри системы на основе формальных политик безопасности [9]. Архитектура FLASK представлена на рисунке 3.

В отличие от MILS, фокус FLASK смещён с изоляции компонентов на принятие решений о допустимости операций.

Все обращения субъектов к объектам системы проходят через:

– модуль принятия решений безопасности (Security Decision Point);

– модуль исполнения решений (Security Enforcement Point).

Политики безопасности формализуются и могут изменяться без модификации прикладного кода.

Совместное использование MILS и FLASK обеспечивает как пространственную изоляцию компонентов, так и строгий контроль логических взаимодействий.

Прикладной уровень реализации методологии кибериммунитета, ориентированный на инженерное формирование устойчивости информационных систем за счёт архитектурных, программных и аппаратных решений представляет собой конструктивную безопасность. В рамках данного подхода безопасность рассматривается не как совокупность внешних защитных механизмов, а как системное свойство, заложенное в конструкцию системы [2].

Рисунок 1 — Архитектурные принципы кибериммунитета: минимизация доверия, изоляция компонентов и контроль взаимодействий

В отличие от традиционных моделей, основанных на реагировании на инциденты, конструктивная безопасность предполагает путём ограничения доверия, изоляции компонентов и строгого контроля взаимодействий.

В основе конструктивной безопасности лежит многоуровневая архитектурная модель, в которой каждый уровень выполняет строго определённую функцию и имеет ограниченную зону ответственности.

Ключевые уровни:

– аппаратный уровень (механизмы изоляции, доверенной загрузки);

– системное ядро (микроядерные и separation-kernel архитектуры);

– прикладные компоненты;

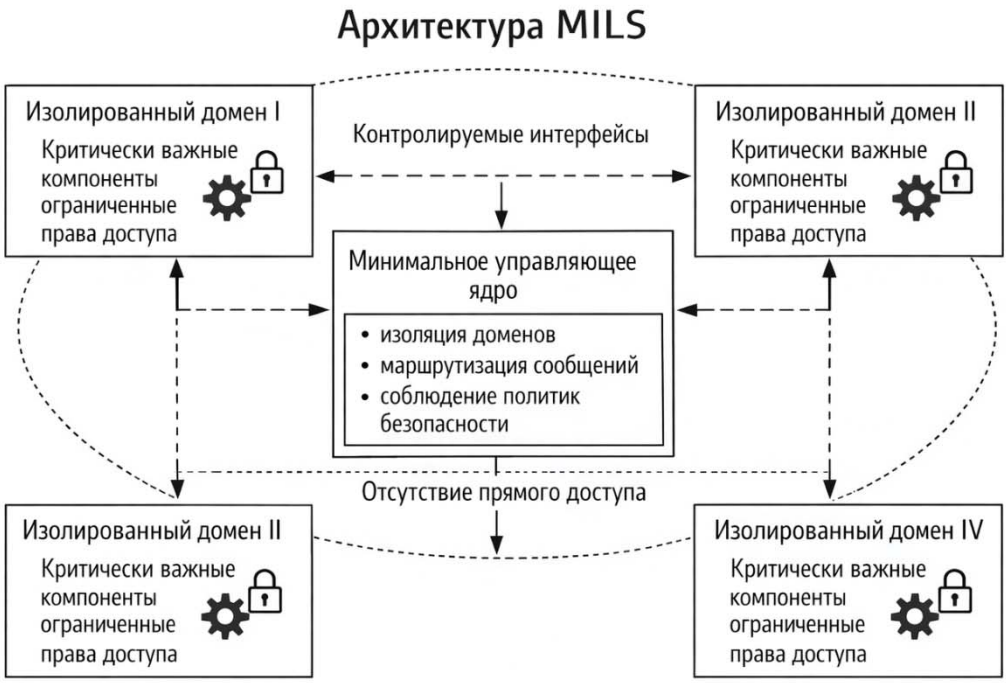

Рисунок 2 — Архитектура MILS: изолированные домены безопасности и минимальное ядро управления.

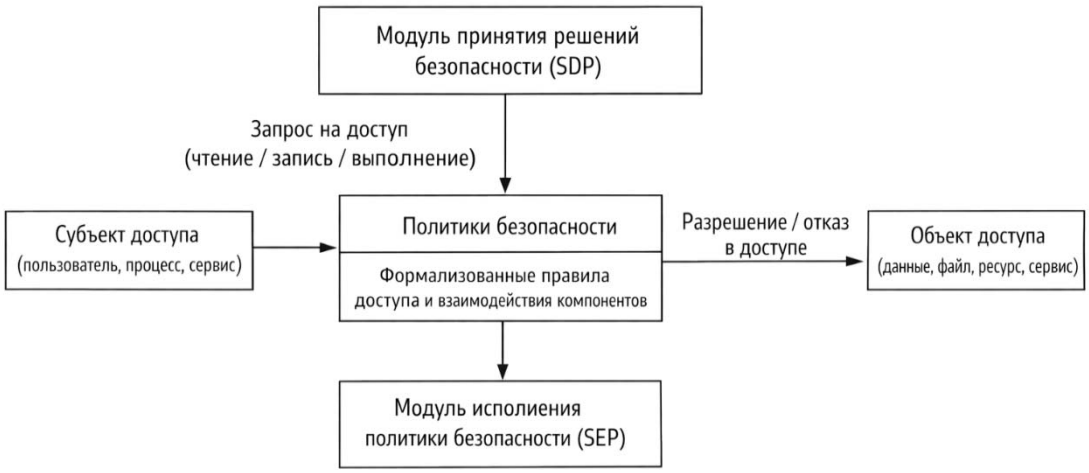

Рисунок 3 — Архитектура FLASK: централизованный контроль доступа и потоков информации.

– политики безопасности и контроль доступа.

Многослойная архитектура конструктивной безопасности с ее основными элементами представлена на рисунке 4.

Данная модель позволяет исключить избыточную функциональность из доверенной вычислительной базы и повысить предсказуемость поведения системы в условиях атак.

Одним из ключевых принципов конструктивной безопасности является минимизация доверенной вычислительной базы (Trusted Computing Base, TCB). В TCB включаются только те компоненты, от корректности работы которых непосредственно зависит безопасность системы [5].

Система проектируется в виде набора изолированных модулей:

– каждый модуль выполняет ограниченный набор функций;

– прямые связи между модулями запрещены;

– взаимодействие осуществляется через контролируемые интерфейсы.

Сокращение TCB снижает вероятность критических уязвимостей.

Модульность и декомпозиция позволяют локализовать ошибки и предотвратить каскадное распространение атак.

В конструктивной безопасности доступ к ресурсам системы предоставляется строго в соответствии с принципом наименьших привилегий. Каждый субъект (пользователь, процесс, сервис) получает только те права, которые необходимы для выполнения текущей задачи [4].

Доступ:

– предоставляется динамически;

– может быть отозван в любой момент;

– зависит от контекста выполнения.

Существенным отличием конструктивной безопасности от традиционных подходов является формализуемость политик безопасности. Правила взаимодействия компонентов описываются в виде формальных моделей, что позволяет:

– анализировать корректность архитектуры;

– выявлять противоречия в политиках;

– применять методы формальной верификации [8].

Использование формальных политик особенно важно для критически важных и высоконадежных систем.

Принципы конструктивной безопасности находят прямое отражение в архитектуре нулевого доверия (Zero Trust), формализованной в NIST SP 800-207 [10]. В 2025 году данный подход стал базовым стандартом защиты от ИИ-ориентированных атак, что подтверждается современными исследованиями и отраслевыми отчётами.

Основные принципы архитектуры нулевого доверия закреплены в ISO/IEC 27001:2022, IEC 62443 и российских ГОСТ [11]–[14].

Таким образом, конструктивная безопасность выступает связующим звеном между теорией кибериммунитета и нормативной базой.

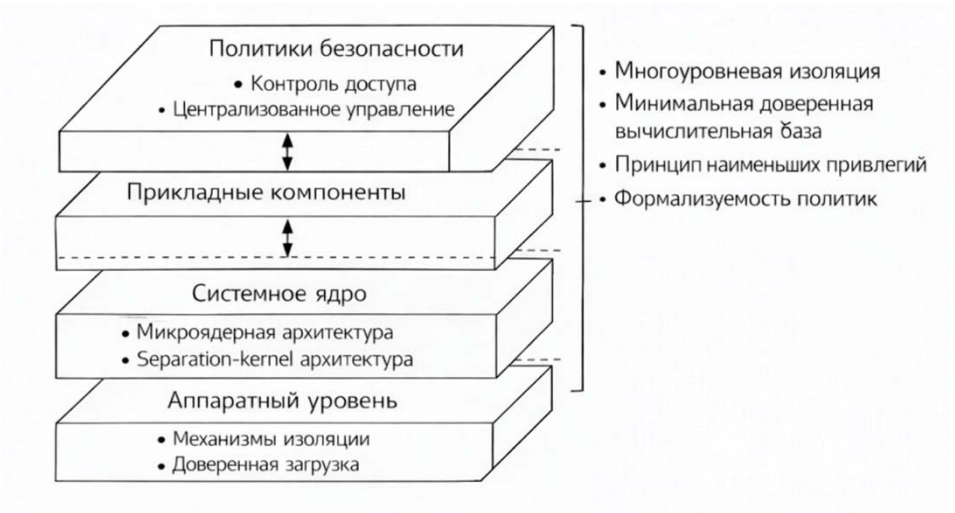

Рисунок 4 — Обобщённая архитектура конструктивной безопасности

Включение методологии кибериммунитета в образовательные программы по направлению 10.05.01 «Компьютерная безопасность», реализуемые в Оренбургский государственный университет, представляется обоснованным с точки зрения как современных требований отрасли, так и задач инженерного образования.

В отличие от традиционного обучения, ориентированного на изучение отдельных средств защиты, преподавание кибериммунитета позволяет выстроить учебный процесс вокруг архитектурного проектирования защищённых систем. Такой подход способствует формированию у студентов целостного представления о безопасности как системном свойстве, а не как совокупности разрозненных механизмов.

С педагогической точки зрения методология кибериммунитета может быть интегрирована в учебный процесс на следующих уровнях:

– теоретическом, через изучение архитектурных принципов, моделей доверия, концепций MILS, FLASK и Zero Trust;

– практическом, через анализ архитектур информационных систем, моделирование угроз и разработку формализованных политик безопасности;

– проектном, через выполнение курсовых и выпускных работ, ориентированных на проектирование кибериммунных систем.

Особое значение имеет использование архитектурных схем и формальных моделей, которые позволяют студентам наглядно прослеживать взаимосвязь между функциональностью системы и её уровнем безопасности. Это способствует развитию аналитического и инженерного мышления, а также формированию навыков принятия проектных решений с учётом ограничений безопасности.

Таким образом, преподавание кибериммунитета и конструктивной безопасности в рамках образовательных программ ОГУ может рассматриваться как эффективный инструмент подготовки специалистов, способных проектировать устойчивые к современным и перспективным киберугрозам информационные системы.

Методология кибериммунитета и концепция конструктивной безопасности отражают современный этап развития информационной безопасности, ориентированный на архитектурную устойчивость систем. Переход от реактивных мер защиты к проектированию безопасных систем является необходимым условием обеспечения безопасности в условиях роста сложности и масштабов киберугроз.

Для подготовки специалистов и бакалавров на информационных направлениях изучение данных подходов имеет фундаментальное значение и способствует формированию системного инженерного мышления.

26.11.2025

Список литературы:

1. Шнайер, Б. Прикладная криптография: протоколы, алгоритмы и исходные тексты на языке С / Б. Шнайер. — 2-е изд. — СПб.: Питер, 2019. — 784 с.
2. Андерсон, Р. Инженерия безопасности компьютерных систем / Р. Андерсон. — М.: Техносфера, 2020. — 832 с.
3. Bishop, M. Computer Security: Art and Science / M. Bishop. — 2nd ed. — Boston: Addison-Wesley, 2018. — 1248 p.
4. Saltzer, J. H. The protection of information in computer systems / J. H. Saltzer, M. D. Schroeder // Proceedings of the IEEE. — 1975. — Vol. 63, No. 9. — P. 1278–1308.
5. Lampson, B. W. Protection / B. W. Lampson // ACM SIGOPS Operating Systems Review. — 1974. — Vol. 8, No. 1. — P. 18–24.
6. Kaspersky Lab. Cyber Immunity: A New Paradigm for Secure Systems Design. — 2020. — URL: https://www.kaspersky.com/cyber-immunity (дата обращения: 10.01.2026).
7. Greve, D. A separation kernel formal security policy / D. Greve, M. Wilding // Proceedings of the High Assurance Systems Engineering Symposium. — Washington: IEEE, 2002. — P. 13–22.
8. Rushby, J. Design and verification of secure systems / J. Rushby // ACM SIGOPS Operating Systems Review. — 1981. — Vol. 15, No. 5. — P. 12–21.
9. Spencer, R. The FLASK security architecture: system support for diverse security policies / R. Spencer, S. Smalley, P. Loscocco, M. Hibler, D. Andersen, J. Lepreau // Proceedings of the 8th USENIX Security Symposium. — Washington, 1999. — P. 123–139.
10. NIST Special Publication 800-207. Zero Trust Architecture. — Gaithersburg: National Institute of Standards and Technology, 2020. — 58 p.
11. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. — Geneva: ISO, 2022.
12. IEC 62443-3-3:2013. Industrial communication networks — Network and system security — Part 3-3: System security requirements and security levels. — Geneva: IEC, 2013.
13. ГОСТ Р 57580.1–2017. Безопасность финансовых (банковских) операций. Защита информации. Общие положения. — М.: Стандартинформ, 2018.
14. ГОСТ Р 56939–2016. Защита информации. Разработка безопасного программного обеспечения. Общие требования. — М.: Стандартинформ, 2017.

15. ФСТЭК России. Методические рекомендации по обеспечению безопасности информации при разработке программного обеспечения. — М.: ФСТЭК России, 2021. — 36 с.

References:

1. Schneier B. (2019) *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. 2nd ed. St. Petersburg: Piter, 784 p. (In Russ.)
2. Anderson R. (2020) *Security Engineering: A Guide to Building Dependable Distributed Systems*. Moscow: Technosphere, 832 p. (In Russ.)
3. Bishop M. (2018) *Computer Security: Art and Science*. 2nd ed. Boston: Addison-Wesley, 1248 p.
4. Saltzer J. H. and Schroeder M. D. (1975) The protection of information in computer systems. *Proceedings of the IEEE*, vol. 63, no. 9, pp. 1278–1308.
5. Lampson B. W. (1974) Protection. *ACM SIGOPS Operating Systems Review*, vol. 8, no. 1, pp. 18–24.
6. Kaspersky Lab. Cyber Immunity: A New Paradigm for Secure Systems Design (2020). Available at: https://www.kaspersky.com/cyber-immunity (accessed 10 January 2026).
7. Greve D. and Wilding M. (2002) A separation kernel formal security policy. *Proceedings of the High Assurance Systems Engineering Symposium*. Washington: IEEE, pp. 13–22.
8. Rushby J. (1981) Design and verification of secure systems. *ACM SIGOPS Operating Systems Review*, vol. 15, no. 5, pp. 12–21.
9. Spencer R., Smalley S., Loscocco P., Hibler M., Andersen D. and Lepreau J. (1999) The FLASK security architecture: system support for diverse security policies. *Proceedings of the 8th USENIX Security Symposium*. Washington, pp. 123–139.
10. NIST Special Publication 800-207. Zero Trust Architecture (2020). Gaithersburg: National Institute of Standards and Technology, 58 p.
11. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection (2022). *Information security management systems*. Requirements. Geneva: ISO.
12. IEC 62443-3-3:2013. Industrial communication networks (2013). *Network and system security.* Part 3-3: System security requirements and security levels. Geneva: IEC.
13. GOST R 57580.1–2017. Security of Financial (Banking) Operations. Information Protection. General Provisions. Moscow: Standartinform, 2018. (In Russ.)
14. GOST R 56939–2016. Information Protection. Secure Software Development. General Requirements. Moscow: Standartinform, 2017. (In Russ.)
15. FSTEC of Russia. Methodological Guidelines for Ensuring Information Security in Software Development. Moscow: FSTEC of Russia, 2021. 36 p. (In Russ.)

Сведения об авторе:

Влацкая Ирина Валерьевна, заведующий кафедрой компьютерной безопасности
и математического обеспечения информационных систем
Института математики и информационных технологий
Оренбургского государственного университета, кандидат технических наук, доцент