УДК: 004.056
DOI: 10.30987/article_5cf2d22c9dcd72.20436206

А.П. Горлов, М.Ю. Рытов, Д.А. Лысов

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ОЦЕНКИ ЭФФЕКТИВНОСТИ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

В статье рассматривается процесс автоматизации оценки эффективности программно-аппаратных средств защиты информации, путем создания автоматизированной системы. Основными функциями предлагаемой системы являются: проведение аудита информационной безопасности, формирование модели угроз ИБ, формирование рекомендаций по созданию программно-аппаратной системы защиты информации, формирование организационно-технической документации.

Ключевые слова: *информационная безопасность, защита информации, программно-аппаратная защита, программно-аппаратные средства защиты информации.*

A.P. Gorlov, M.Yu. Rytov, D.A. Lysov

AUTOMATED SYSTEM FOR ESTIMATION-EFFICIENCYSOFTWARE MEANS OF IN-FORMATION PROTECTION

The article discusses the process of automating the assessment of the effectiveness of software and hardware information protection by creating an automated system. The main functions of the proposed system are: conducting an information security audit, forming an information security threat model, making recommendations for creating a software and hardware information protection system, and creating organizational and technical documentation.

Keywords: *information security, information protection, software and hardware protection, software and hardware information protection.*

Введение

На сегодняшний день проблема защиты конфиденциальной информации стоит особенно остро. Ущерб от реализации угроз компьютерным системам и обрабатываемой в них конфиденциальной информации превышает миллионы рублей.

По статистике за 2018 год на территории РФ зафиксировано около 300 тысяч преступлений в сфере информационной безопасности. К этим преступлениям относятся несанкционированный доступ к конфиденциальной информации, утечка и разглашение атрибутов доступа к подсистемам компьютерных систем, создание, использование или распространение вредоносных программ для ЭВМ или машинных носителей с такими программами.

Компьютерная система – любое устройство или группа взаимосвязанных, или смежных устройств, одно или более из которых, действуя в соответствии с программой, осуществляет автоматизированную обработку данных.

Объектом информатизации называется совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов, в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведений конфиденциальных переговоров.

Отсутствие на объектах информатизации программно-аппаратных систем защиты информации приводит к утечке конфиденциальной информации, так как разработка и внедрение таких систем является достаточно сложной и затратной процедурой. В общем случае на компьютерную систему влияет ряд факторов, который можно условно разделить

на две категории: требования законодательства и стандартов в области защиты информации, а также различные угрозы информационной безопасности. Автоматизированная система оценки эффективности программно-аппаратных средств защиты информации позволит привести КС в соответствие установленным требованиям, противостоять актуальным угрозам, снизить трудоемкость работ, сэкономить время и значительно сократить материальные затраты на проведение аудита и разработку программно-аппаратных систем защиты информации.

1. Постановка задачи

Ввиду этого разработка системы автоматизированной оценки эффективности программно-аппаратных средств защиты представляется актуальной. На данный момент автоматизированная оценка уровня информационной безопасности производится исключительно по стандартам ISO, однако в РФ более распространена организационно-распорядительная документация.

В предлагаемом подходе в основу положена оценка защищенности объекта информатизации согласно положениям законодательной базы РФ, требованиям государственных стандартов, а также проверка наличия организационно-технической документации, регламентирующей защиту компьютерных систем.

Основной задачей, разрабатываемой автоматизированной системы является выявление уязвимостей существующих систем обработки и защиты информации. В качестве входных данных используются данные о компьютерных системах. Данные вводятся на основе специально разработанных опросных анкет.

2. Решение

Алгоритм работы АС:

1. Ввод исходных данных.
2. Формирование информационной модели компьютерной системы, определение целей и задач по защите информации.
3. Оценка состояния защищенности объекта информатизации.
4. Формирование модели угроз информационной безопасности.
5. Формирование рекомендаций по совершенствованию системы защиты информации.
6. Формирование организационно-технической документации.

Преимуществом данной методики является возможность снизить трудоемкость работ, сократить временные и материальные затраты на проведение оценки уровня информационной безопасности, повысить качество проектных решений.

Структурно-функциональная схема, разработанной автоматизированной системы представлена на рис. 1.

Ввод исходных данных представляет собой заполнение опросных анкет, которые позволят выявить вид обрабатываемой информации, существующие программно-аппаратные средства защиты информации, угрозы ИБ, уязвимости системы защиты информации, а также прочие данные позволяющие составить информационную модель объекта информатизации.

Следующим этапом является оценка состояния защищенности компьютерной системы. Выделяется 3 основных направления оценки защищенности:

1. Оценка на соответствие требованиям стандартов (ГОСТ, СТР-К, ISO).
2. Определение наличия программно-аппаратных средств защиты информации на объекте информатизации.
3. Выявление организационно-технической документации, регламентирующей защищенную обработку конфиденциальной информации.

По результатам данного этапа формируется отчет о состоянии защищенности компьютерной системы.

На этапе формирования модели угроз информационной безопасности формируется описание системы обработки информации, выявляются пользователи данной системы, определяется уровень исходной защищенности, степень актуальности угроз, рассчитывается вероятность реализации угроз.

Актуальность рисков определяется исходя из типа обрабатываемой информации, объема обрабатываемых в системе данных, структуры информационной системы, режиму обработки данных и т.д.

Рис. 1. Структурно-функциональная схема автоматизированной системы

Однако для того чтобы определить актуальность угроз для данного объекта информатизации целесообразно выделить критерии актуальности каждой конкретной угрозы. Так для угрозы сетевой атаки можно выделить такие критерии актуальности как наличие доступа к глобальной сети, наличие в структуре локальной вычислительной сети средств межсетевого экранирования, антивирусной защиты и т.д.

Основываясь на выделенных критериях актуальности возможно формализовать расчет вероятности реализации угроз:

$$P(i) = \frac{\sum f(j)}{N} * 100\%$$

$P(i)$ – вероятность реализации i-ой угрозы, $f(j)$ – функция расчета влияния j-го критерия на защищенность системы от i-ой угрозы, N – кол-во факторов.

На данном этапе результатом работы является модель угроз на основании которой можно выделить оптимальные средства защиты от наиболее актуальных и вероятных угроз.

Для обеспечения защиты от таких угроз предусмотрен процесс выборки программных

и аппаратных средств защиты информации из базы данных. Выборка производится исходя из стоимости средств защиты и оптимальных технических характеристик необходимых для обеспечения требуемого уровня защищенности.

Формализацию процесса формирования модели угроз можно представить в виде кортежа:

$$M = < Di, T, Th, Ka, P >,$$

где D_i– уровень исходной защищенности, T – тип системы обработки информации, Th – угрозы информационной безопасности, K_a– критерии актуальности угроз, P – вероятность реализации угроз

Следующим этапом является формирование рекомендаций по совершенствованию системы защиты информации. Рекомендации разделяются на 4 основных раздела:

1. Рекомендации по антивирусной защите информации.
2. Рекомендации по защите информации от несанкционированного доступа (НСД).
3. Рекомендации по применению средств межсетевого экранирования.
4. Рекомендации по применению средств обнаружения вторжений.

По каждому разделу приводится ряд мер, выполнение которых необходимо для защиты от выявленных угроз. Так же на данном этапе происходит подбор оптимальных средств программно-аппаратной защиты информации исходя из допустимой стоимости и набора необходимых характеристик.

Заключительным этапом является формирование организационно-технической документации, регламентирующей защиту конфиденциальной информации.

На данном этапе производится оценка наличия организационно-технической документации на объекте, выявляются недостающие документы, если необходимо, производится сбор дополнительных данных необходимых для формирования дополнительных документов.

В качестве выходных данных по результатам работы данного блока является комплект организационно-технической документации, регламентирующей эксплуатацию программно-аппаратных средств защиты.

Результаты работы автоматизированной системы представлены на рис.2.

Рис.2. Результаты работы АС

Заключительным этапом является формирование организационно-технической документации, регламентирующей защиту конфиденциальной информации.

На данном этапе производится оценка наличия организационно-технической документации на объекте, выявляются недостающие документы, если необходимо, производится сбор дополнительных данных необходимых для формирования дополнительных документов.

В качестве выходных данных по результатам работы данного блока является комплект организационно-технической документации, регламентирующей эксплуатацию программно-аппаратных средств защиты.

Результаты работы автоматизированной системы представлены на рис.2.

В результате проведенного вычислительного и имитационного моделирования полечено 255 вариантов построения программно-аппаратной системы защиты информации (рис. 3).

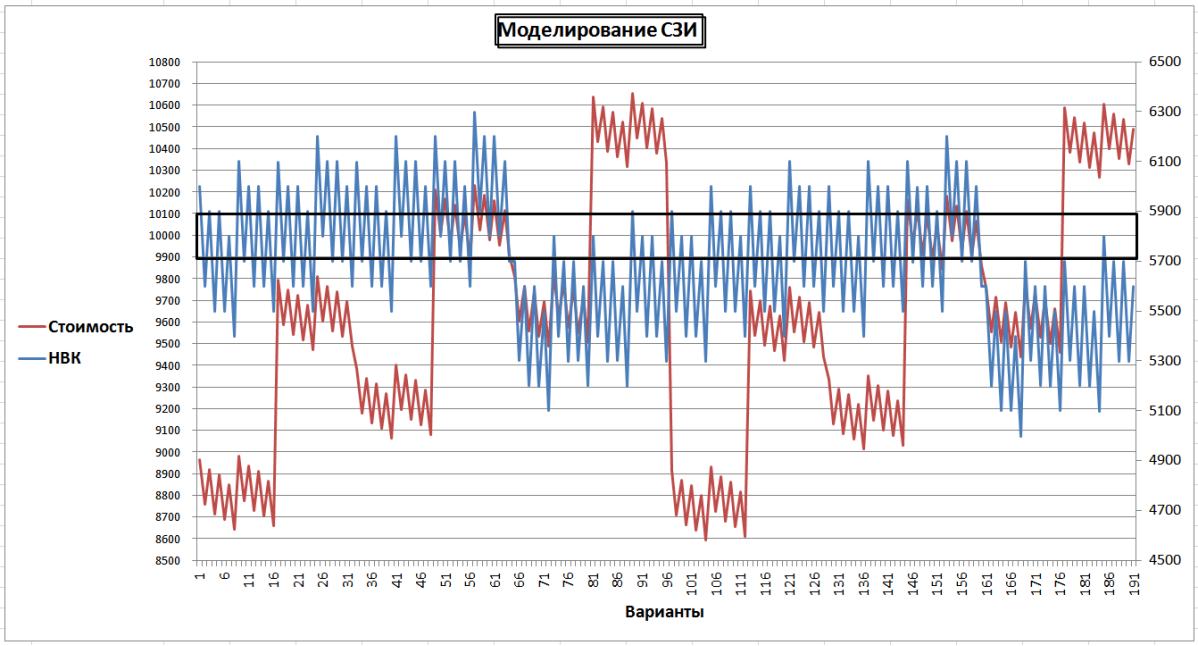

Рис. 3. Результаты имитационного моделирования

Учитывая финансовую целесообразность проводимых мероприятий, был выбраны 5 наиболее эффективных вариантов построения программно-аппаратной системы защиты информации на основе разработанного критерия эффективности (таблица 1).

Таблица 1. Варианты построения ПАЗИ

Номер варианта защиты	Накопленный весовой коэффициент (W)	Стоимость (C)	Набор средств защиты
№50	5799,763	10006	$V_1, V_4, V_7, V_8, V_{10}, V_{12}, V_{15}, V_{16}$
№52	5698,114	9961	$V_1, V_4, V_7, V_8, V_{10}, V_{13}, V_{15}, V_{16}$
№54	5698,231	9936	$V_1, V_4, V_7, V_8, V_{11}, V_{12}, V_{15}, V_{16}$
№146	5696,731	9957	$V_2, V_5, V_7, V_8, V_{10}, V_{12}, V_{15}, V_{16}$
№158	5699,865	9904	$V_2, V4, V_7, V_9, V_{11}, V_{12}, V_{15}, V_{16}$

Было произведено моделирование работы выбранных вариантов построения ПАЗИ для 100 (рис. 4) и 10000 (рис.5) тактов работы построенной математической модели на основе раскрашенных сетей Петри, в результате которого было определено что значение накопленного весового коэффициента меняется с течением времени, что свидетельствует об адекватности модели, а также был определен наиболее эффективный набор технических средств защиты информации.

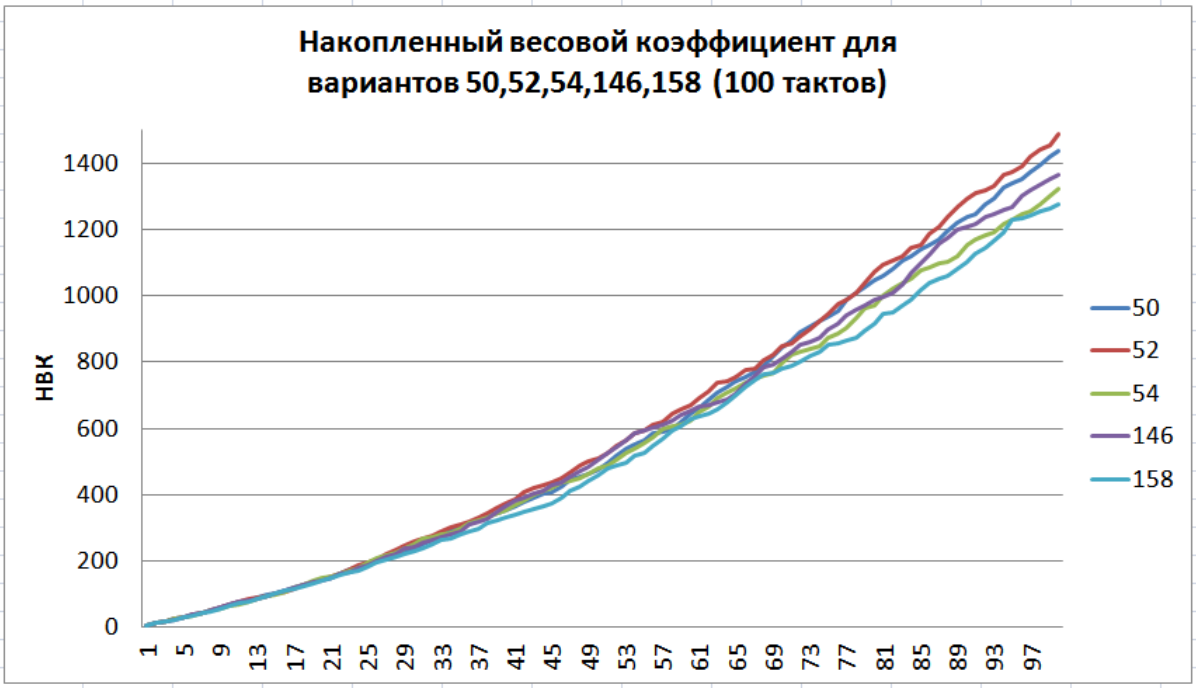

Рис. 4. Накопленный весовой коэффициент для вариантов защиты № 50, 52, 54, 146, 158 для 100 тактов

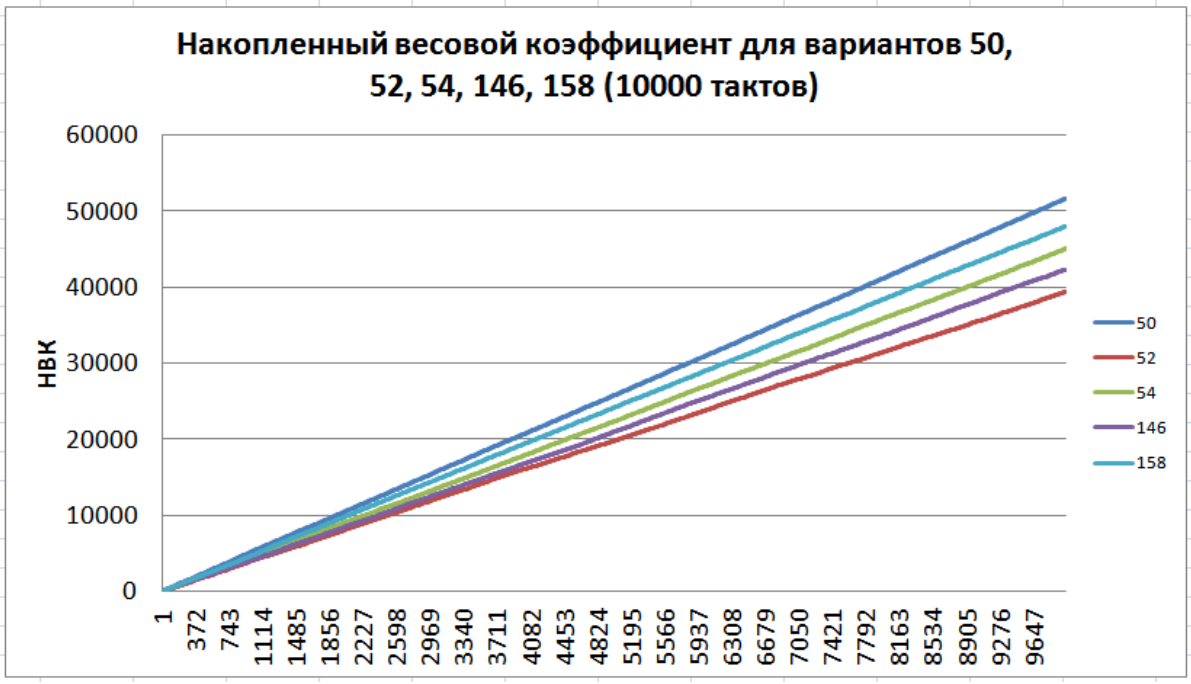

Рис. 5. Накопленный весовой коэффициент для вариантов защиты № 50, 52, 54, 146, 158 для 10000 тактов

Заключение

Таким образом разработанная автоматизированная система оценки эффективности программно-аппаратных средств защиты информации позволяет в автоматизированном

режиме построить модель угроз информационной безопасности, сформировать организационно-техническую документацию регламентирующую защиту конфиденциальной информации, а также сформировать рекомендации по усовершенствованию программно-аппаратной системы защиты информации. Применение данной системы позволит значительно сократить временные и материальные затраты на проведение аудита информационной безопасности и разработку дополнительных мер защиты информациипо сравнению с неавтоматизированным проектированием программно-аппаратной системы защиты информации.

Список литературы:

1. Аверченков, В.И. Автоматизация защиты персональных данных в ВУЗе / В.И. Аверченков, М.Ю. Рытов, В.А. Шкаберин, О.М. Голембиовская //Известия Международной ассоциации славянских вузов, № 1, 2011 г. – с. 126–134.
2. Иванько, А.Ф. Автоматизация проектирования систем и средств управления: учебное пособие / А.Ф. Иванько, М.А. Иванько, В.Г. Сидоренко, Г.Б. Фалк. – М.: Изд–во МГУП, 2001. – 148 с.
3. Андрианов, В.В. Обеспечение информационной безопасности бизнеса / В.В. Андрианов, С.Л.Зефиров, В.Б.Голованов, Н.А. Голдуев под ред. А.П. Курило – М.: Альпина Паблишерз, 2011.
4. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка), ФСТЭК,2008
5. Рытов, М.Ю. Автоматизация процесса оценки состояния защищенности объекта информатизации с использованием раскрашенных сетей Петри от утечки информации/ М.Ю. Рытов, А.П. Горлов, В.Т. Еременко// Информация и безопасность. – 2015. – №1. – С. 123–126.
6. Климов, С.М. Противодействие компьютерным атакам. Технологические основы: электронное учебное издание./ А.В. Астрахов, С.М. Климов, М.П. Сычев // – М.: МГТУ имени Н.Э. Баумана, 2013. – 108 с.
7. Лысов Д.А . Авторизация пользователей на основе комплексного применения методов распознавания лиц [Текст + Электронный ресурс] / Рытов М.Ю., Шкаберин В.А., Лысов Д.А., Горлов А.П. // Информация и безопасность №1, 2016.-с. 106-109;
8. Лысов Д.А. Автоматизация процесса оценки эффективности комплексных систем защиты информации промышленных предприятий при одновременной реализации угроз [Текст + Электронный ресурс] / Рытов М.Ю., Горлов А.П., Лысов Д.А., Вестник Брянского государственного технического университета №4, 2016.-с. 199-206
9. Лысов Д.А. Методические аспекты аутентификации пользователей СКУД посредством применения технологий распознавания лиц [Текст + Электронный ресурс] /Голембиовская О.М., Горлов А.П., Лексиков Е.В., Лысов Д.А., Рытов М.Ю.// Информационные системы и технологии №6(110), 2018.-с. 116-121;
10. Ляско, В.И. Стратегическое планирование развития предприятия: учебное пособие для вузов / В.И. Ляско // – М.: Издательство «Экзамен», серия

References:

1. Averchenkov, V.I. Automation of personal data protection in the university / V.I. Averchenkov, M.Yu. Rytov, V.A. Shkaberin, OM Golembiovskaya // Proceedings of the International Association of Slavic Higher Education Institutions, № 1, 2011 - p. 126-134;
2. Ivanko, A.F. Automation of systems design and management tools: a tutorial / A.F. Ivanko, M.A. Ivanko, V.G. Sidorenko, G.B. Falk - M .: Publishing House of MGUP, 2001. - 148 p;
3. Andrianov, V.V. Ensuring information security of business / V.V. Andrianov, S.L. Zefirov, V.B.Golovanov, N.A. Golduev ed. A.P. Kurylo - M .: Alpina Publishers, 2011;
4. The basic model of threats to the security of personal data when they are processed in personal data information systems (extract), FSTEC, 2008;

5. Rytov, M.Yu. Automating the process of assessing the state of security of an informatization object using colored Petri nets from information leakage / M.Yu. Rytov, A.P. Gorlov, V.T. Eremenko // Information and Security. - 2015. - №1. - pp. 123–126;

6. Klimov, S.M. Countering computer attacks. Technological background: electronic educational edition. / A.V. Astrakh, S.M. Klimov, M.P. Sychev // - M .: MSTU named after NE Bauman, 2013. - 108 p;
7. Lysov D.A. Authorization of users on the basis of the integrated application of the methods of face recognition [Text + Electronic Resource] / Rytov M.Yu., Shkaberin VA, Lysov DA, Gorlov AP // Information and security №1, 2016.- p. 106-109;
8. Lysov D.A. Automating the process of evaluating the effectiveness of integrated information security systems for industrial enterprises while simultaneously implementing threats [Text + Electronic Resource] / Rytov M.Yu., Gorlov AP, Lysov DA, Bulletin of Bryansk State Technical University №4, 2016 .-with. 199-206;
9. Lysov D.A. Methodical aspects of authentication of access control systems through the use of facial recognition technologies [Text + Electronic Resource] / Golembiovskaya OM, Gorlov AP, Leksikov EV, Lysov DA, Rytov M.Yu.// Information systems and technologies №6 (110), 2018.- p. 116-121;

10. Lyasko, V.I. Strategic development planning of the enterprise: a textbook for universities / V.I. Lyas-ko // - Moscow: Examination Publishing House, “Study Guide

«Учебное пособие для вузов»), 2005. – 288 с.
11. Нестерук, Г.Ф. К разработке модели адаптивной защиты информации / Г.Ф. Нестерук, А.А. Молдовян, Л.Г. Осовецкий, Ф.Г. Нестерук, Р.Ш. Фархутдинов // Вопросы защиты информации. 2005, № 3. С. 11 – 16.

for Universities" series), 2005. - 288 p.;
11. Nesteruk, G.F. On the development of a model of adaptive information security / G.F. Nesteruk, A.A. Moldovyan, L.G. Osovetsky, F.G. Nesteruk, R.Sh. Farkhutdinov // Information Security Issues. 2005, No. 3. P. 11 - 16..

Статья поступила в редколлегию 03.04.19.
Рецензент: к.т.н., доцент Брянского государственного технического университета Дергачев К.В.
Статья принята к публикации 30.04.19.

Сведения об авторах:

Горлов Алексей Петрович
Доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «Брянский государственный технический университет», кандидат технических наук
тел.: +7 (980) 302 53 80
E-mail: apgorlov@gmail.com

Рытов Михаил Юрьевич
Заведующий кафедрой «Системы информационной безопасности» ФГБОУ ВО «Брянский государствен-ный технический университет», доцент, кандидат технических наук
тел.: +7 (910) 330 02 37
E-mail: rmy@tu-bryansk.ru

Лысов Дмитрий Андреевич
Ассистент кафедры Системы информационной безопасности» ФГБОУ ВО «Брянский государственный технический университет»
тел.: +7 (910) 330 54 33
E-mail: lysovdmitriia@gmail.com

Information about authors:

Gorlov Alexey Petrovich
Associate Professor of the Department of Information Security Systems at FSBEI HE "Bryansk State Technical University", Candidate of Technical Sciences
tel.: +7 (980) 302 53 80
E-mail: apgorlov@gmail.com

Rytov Mikhail Yurievich
Head of the Department of Information Security Systems at FSBEI HE "Bryansk State Technical University", Associate Pro-fessor, Candidate of Technical Sciences
tel.: +7 (910) 330 02 37
E-mail: rmy@tu-bryansk.ru

Lysov Dmitry Andreevich
Assistant of the Department of Information Security Systems at FSBEI HE "Bryansk State Technical University"
tel.: +7 (910) 330 54 33
E-mail: lysovdmitriia@gmail.com