**ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ**
**INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS**

**УДК 004.056**
**DOI:** 10.21822/2073-6185-2022-49-4-97-103 Обзорная статья / Review article

# К вопросу анализа нормативно-правовых документов по информационной безопасности автоматизированных систем органов внутренних дел Российской Федерации для оценки уровня их защищенности

**Е.А. Рогозин, И.Г. Дровникова, А.О. Ефимов, В.Р. Романова**
Воронежский институт МВД России,
394065, г. Воронеж, пр. Патриотов, 53, Россия

**Резюме. Цель.** При решении научной задачи, связанной с оценкой защищенности автоматизированных систем органов внутренних дел, в частности, при разработке методики количественной оценки защищенных автоматизированных систем органов внутренних дел, первым этапом решения является анализ международных, российских, а также ведомственных нормативно-правовых документов по информационной безопасности (ИБ) автоматизированных систем органов внутренних дел Российской Федерации (АС ОВД РФ), по результатам анализа которых необходимо разработать методику количественной оценки уровня защищенности АС ОВД РФ. **Метод.** В ходе работы произведен анализ международных, российских, а также ведомственных нормативно-правовых документов по информационной безопасности АС ОВД РФ. **Результат.** Получен исчерпывающий список литературы, включающий в себя международные, российские, а также ведомственные нормативно-правовые документы по информационной безопасности АС ОВД РФ. **Вывод.** Анализ международных, российских, а также ведомственных нормативно-правовых документов по информационной безопасности АС ОВД РФ показал, что документы, посвященные защите информации АС ОВД РФ, а также методика количественной оценки уровня защищенности этих систем проработана в недостаточном объеме, в частности, отсутствуют система показателей, а также математические модели и алгоритмы оценки уровня защищенности АС ОВД РФ, что требует значительного совершенствования этих документов.

**Ключевые слова:** оценка уровня защищенности, автоматизированная система, защищенная автоматизированная система, количественная оценка, информационная безопасность

**Для цитирования:** Е.А. Рогозин, И.Г. Дровникова, А.О. Ефимов, В.Р. Романова. К вопросу анализа нормативно-правовых документов по информационной безопасности автоматизированных систем органов внутренних дел Российской Федерации для оценки уровня их защищенности. Вестник Дагестанского государственного технического университета. Технические науки. 2022; 49(4):97-103. DOI:10.21822/2073-6185-2022-49-4-97-103

# On the issue of analysis of legal documents on information security of automated systems of internal affairs bodies of the Russian Federation to assess the level of their security

**E.A. Rogozin, I.G. Drovnikova, A.O. Efimov, V.R. Romanova**
Voronezh Institute of the Ministry of Internal Affairs of Russia,
53 Patriotov Str., Voronezh 394065, Russia

**Abstract. Objective.** When solving a scientific problem related to assessing the security of automated systems of internal affairs bodies, in particular, when developing a methodology for quantifying protected automated systems of internal affairs bodies, the first stage of the solution is the analysis of international, Russian, as well as departmental legal documents on information security ( IS) of automated systems of internal affairs bodies of the Russian Federation (AS ATS of the Russian Federation), based on the results of the analysis of which it is necessary to develop a methodology for quantifying the level of security of the ATS of the Russian Federation. **Method.** In the course of the work, an

analysis was made of international, Russian, as well as departmental legal documents on information security of the ATS of the Russian Federation. **Result.** An exhaustive list of literature has been obtained, including international, Russian, as well as departmental legal documents on information security of the RF ATS AS. **Conclusion.** An analysis of international, Russian, as well as departmental legal documents on information security of the ATS of the Russian Federation showed that the documents on the protection of information of the ATS of the Russian Federation, as well as the methodology for quantifying the level of security of these systems, have been developed insufficiently, in particular, they are absent a system of indicators, as well as mathematical models and algorithms for assessing the level of security of the ATS of the Russian Federation, which requires significant improvement of these documents.

**Keywords:** assessment of the level of security, automated system, secure automated system, quantitative assessment, information security

**For citation:** E.A. Rogozin, I.G. Drovnikova, A.O. Efimov, V.R. Romanova. On the issue of analysis of legal documents on information security of automated systems of internal affairs bodies of the Russian Federation to assess the level of their security. Herald of the Daghestan State Technical University. Technical Science. 2022; 49(4): 97-103. DOI:10.21822/2073-6185-2022-49-4-97-103

**Введение.** В настоящее время, существует значительное количество подходов в области защиты информации, в частности в обеспечение информационной безопасности (ИБ) автоматизированных систем (АС) ОВД РФ [10-9]. В связи с этим, появляется необходимость в выборе наиболее подходящих методологий в области ИБ, с помощью которых можно более детально узнать: терминологию в области ИБ; общие подходы к построению ИБ; общепринятые процессы ИБ и рекомендации по их выстраиванию; конкретные меры защиты ИБ; роли и зоны ответственности при построении процессов ИБ; подходы к измерению зрелости процессов ИБ; и т.д. Помимо всего вышеперечисленного, изучение и практическое применение известных методологий дает возможность грамотно обосновывать необходимость применения тех или иных мер ИБ.

Национальные стандарты информационной безопасности – это обязательные или рекомендуемые к выполнению документы, в которых определены подходы к оценке уровня ИБ и установлены требования к безопасным информационным системам [10-18].

Стандарты в области информационной безопасности выполняют следующие важнейшие функции: выработка понятийного аппарата и терминологии в области ИБ; формирование шкалы измерений уровня ИБ; согласованная оценка продуктов, обеспечивающих ИБ; повышение технической и информационной совместимости продуктов, обеспечивающих ИБ; накопление сведений о лучших практиках обеспечения ИБ.

В настоящее время в России наряду с отечественной нормативной базой широко используются международные стандарты в области информационной безопасности. Некоторые международные стандарты по защите информации приняты и введены в действие в России, но эти стандарты не составляют целостной основы для решения проблем информационной безопасности, особенно в части нормативного регулирования, методического и инструментального обеспечения разработки, оценки и сертификации безопасности информационных технологий с учетом современного уровня развития, масштабов и многообразия угроз [1-9].

Международные стандарты описывают следующие задачи: определение целей обеспечения ИБ компьютерных систем; создание эффективной системы управления ИБ; расчет совокупности детализированных не только качественных, но и количественных показателей для оценки соответствия ИБ заявленным целям; применение инструментария обеспечения ИБ и оценки ее текущего состояния.

Нормативно-правовые документы также являются основополагающем в изучении вопроса, связанных с ИБ, в них предусмотрены меры, касающиеся ответственности и наказания за нарушение правил и норм безопасности, а также информация, связанная с повышением осве-

домленности граждан в данной сфере, разработкой и распространением различных защитных технологий и средств [19-27]. В данный перечень источников необходимо включить работы ученых, связанных с обеспечением ИБ, так как проведенный анализ показал, что работ, рассмотренных в данной области много, однако они описаны не в полной мере, что требует дальнейшего анализа [28-36].

**Постановка задачи.** В целях получения необходимого перечня литературных источников, связанных с защитой информации АС ОВД РФ, необходимо произвести анализ международных, российских, а также ведомственных нормативно-правовых документов по информационной безопасности АС ОВД РФ. Данный анализ позволит более детально разобрать задачи, стоящие перед ОВД РФ.

**Методы исследования.** В результате проведенного анализа, получен значительный объем источников, связанных с информационной безопасностью АС ОВД РФ. Ниже будут рассмотрены основополагающие документы, служащие методологической опорой при решении рассматриваемой научной задачи.

Международные стандарты:

1. ГОСТ Р 54581-2011/ISO/IEC TR 15443-1:2005. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 1. Обзор и основы.

Стандарт предназначен для описания методов обеспечения доверия к безопасности, соотнесения их с базовой моделью жизненного цикла объекта и классификации методов обеспечения доверия для получения высокой степени уверенности в функциональных возможностях обеспечения безопасности объекта [1].

2. ГОСТ Р 56045-2014/ISO/IEC TR 27008:2011. Информационная технология. Методы и средства обеспечения безопасности. Рекомендации для аудиторов в отношении мер и средств контроля и управления информационной безопасностью. Стандарт предоставляет руководство по проверке реализации и функционирования мер и средств контроля и управления, включая проверку технического соответствия мер и средств контроля и управления информационных систем, согласно установленным в организации стандартам по информационной безопасности [2].

3. ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Стандарт представляет собой руководство по управлению безопасностью информационных и телекоммуникационных технологий (ИТТ), устанавливает концепцию и модели, лежащие в основе базового понимания безопасности ИТТ, и раскрывает общие вопросы управления, которые важны для успешного планирования, реализации и поддержки безопасности ИТТ [3].

Национальные стандарты:

1. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. Стандарт устанавливает основные термины с соответствующими определениями, применяемые при проведении работ по стандартизации в области защиты информации [11].

2. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Стандарт устанавливает единые функциональные требования к защите средств вычислительной техники (СВТ) от несанкционированного доступа (НСД) к информации; к составу документации на эти средства, а также номенклатуру показателей защищенности СВТ, описываемых совокупностью требований к защите и определяющих классификацию СВТ по уровню защищенности от НСД к информации [10].

3. ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.

Стандарт устанавливает типовые требования, предъявляемые к испытаниям ПС на наличие КВ, в том числе: к составу мероприятий по подготовке и проведению испытаний; к составу, структуре и назначению основных частей программно-аппаратного стенда, обеспечивающего

проведение испытаний; к выбору и использованию методов проведения испытаний; к тестовым программам, обнаруживающим и уничтожающим КВ; к составу и содержанию документации, фиксирующей порядок проведения испытаний и их результаты. Настоящий стандарт предназначен для применения в испытательных лабораториях, проводящих сертификационные испытания ПС на выполнение требований защиты информации [12].

Нормативно-правовые документы:

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Федеральный закон регулирует отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;

2) применении информационных технологий;

3) обеспечении защиты информации.

Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации [24].

2. Закон РФ от 21 июля 1993 г. N 5485-1 «О государственной тайне».

Данный закон устанавливает единые функциональные требования к защите средств вычислительной техники (СВТ) от несанкционированного доступа (НСД) к информации; к составу документации на эти средства, а также номенклатуру показателей защищенности СВТ, описываемых совокупностью требований к защите и определяющих классификацию СВТ по уровню защищенности от НСД к информации [19].

3. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных».

Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов РФ, иными государственными органами, органами местного самоуправления, не входящими в систему органов местного самоуправления муниципальными органами, юридическими лицами, физическими лицами с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации [25].

Работы учёных, связанные с ИБ:

1. Рогозин Е.А. Способ определения комплексного показателя защищенности автоматизированных систем / Е. А. Рогозин, О. В. Ланкин, Д. А. Багаев // Вопросы защиты информации. – 2009. – № 2(85). – С. 8-10.

Предложен способ определения обобщенного показателя защищенности автоматизированных систем и эффективности систем защиты информации от несанкционированного доступа. Вычисление показателя осуществляется с использованием структуры требований, содержащейся в «Общих критериях» и в соответствующем российском аналоге ГОСТ Р 15408-2-2002 [29].

2. Язов Ю.К. Информационные риски в условиях применения технологии виртуализации в информационно-телекоммуникационных системах / Ю. К. Язов, В. Н. Сигитов // Информация и безопасность. – 2013. – Т. 16. – № 3. – С. 403-406.

Приводятся особенности технологии виртуализации, указываются связанные с ними специфические угрозы безопасности информации и информационные риски, обусловленные возможностью реализации таких угроз. Отмечается необходимость разработки новых и совершенствования существующих способов и средств защиты, предназначенных для нейтрализации угроз безопасности информации, обрабатываемой в информационно-телекоммуникационных системах с применением, технологи виртуализации [32].

3. Авсентьев О.С. Обеспечение защиты информации в процессе создания информацион-

ной системы объекта информатизации / О. С. Авсентьев, А. Г. Вальде, Ю. В. Конкин // Вестник Воронежского института МВД России. – 2021. – № 3. – С. 36-48.

Рассматриваются вопросы обеспечения защиты информации, содержащей сведения о видах информации, ее материальных носителях, структурно-функциональных характеристиках информационной системы объекта информатизации и взаимосвязях между его структурными элементами. Учитываются условия, характеризующие динамику выполнения нарушителем действий по добыванию такого рода сведений путем преодоления мер защиты информации информационно-сигнализационной системы контроля и ограничения доступа на территорию проектируемого объекта, а также действий легитимных пользователей по блокированию утечки за счет применения превентивных мер защиты этой информации. Предложен показатель оценки защищенности информации от утечки. Обоснован подход к разработке математической модели для расчета этого показателя [36].

**Вывод.** Анализ международных, российских, а также ведомственных нормативно-правовых документов по информационной безопасности АС ОВД РФ показал, что документы, посвященные защите информации АС ОВД РФ, а также методика количественной оценки уровня защищенности этих систем проработана в недостаточном объеме, в частности, отсутствуют система показателей, а также математические модели и алгоритмы оценки уровня защищенности АС ОВД РФ, что требует значительного совершенствования этих документов.

**Библиографический список:**

1. ГОСТ Р 54581-2011 / ISO/IEC TR 15443-1:2005. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 1. Обзор и основы. 2012. 27 с.
2. ГОСТ Р 54582-2011 / ISO/IEC TR 15443-2:2005. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 2. Методы доверия. 2019. 52 с.
3. ГОСТ Р 54583-2011 / ISO/IEC TR 15443-3:2007. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 3. Анализ методов доверия. 2011. 54 с.
4. ГОСТ Р 56045-2014 / ISO/IEC TR 27008:2011. Информационная технология. Методы и средства обеспечения безопасности. Рекомендации для аудиторов в отношении мер и средств контроля и управления информационной безопасностью. 2014. 44 с.
5. ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. 2006. 23 с.
6. ГОСТ Р ИСО 7498-1-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель. 2006. 62 с.
7. ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. 1999. 39 с.
8. ГОСТ Р ИСО/МЭК ТО 13335-5-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети. 2006. 33 с
9. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. 2012. 56 с.
10. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. 2006. 10 с.
11. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения // М.: Федеральное агентство по техническому регулированию и метрологии. 2006. 12 с.
12. ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. 1998. 8 с.
13. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. 2006. 11 с.
14. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. 2014. 18 с.
15. ГОСТ Р 52069.0-2013. Защита информации. Система стандартов. Основные положения. 2013. 15 с.
16. ГОСТ Р 52447-2005. Защита информации. Техника защиты информации. Номенклатура показателей качества. 2005. 27 с.
17. ГОСТ Р 52448-2005. Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения. 2005. 19 с.
18. ГОСТ Р 52633.0-2006. Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации. 2006. 24 с.
19. Закон РФ от 21 июля 1993 г. N 5485-1 «О государственной тайне».
20. Федеральный закон от 27 декабря 2002 г. N 184-ФЗ «О техническом регулировании».
21. Федеральный закон от 07 июля 2003 г. N 126-ФЗ «О связи».
22. Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне».

23. Федеральный закон от 19 декабря 2005 г. N 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
24. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
25. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных».
26. Федеральный закон от 28 декабря 2010 г. N 390-ФЗ «О безопасности».
27. Федеральный закон от 06 апреля 2011 г. N 63-ФЗ «Об электронной подписи».
28. Применение метода топологического преобразования стохастических сетей для оценки эффективности средств защиты / В. В. Баранов, А. М. Крибель, О. С. Лаута, А. П. Нечепуренко // Актуальные проблемы обеспечения информационной безопасности : труды Межвузовской научно-практической конференции, Самара, 20–24 мая 2017 года. – Самара: Инсома-Пресс, 2017. – С. 47-52. – EDN ZAMPAR.
29. Рогозин Е. А. Способ определения комплексного показателя защищенности автоматизированных систем / Е. А. Рогозин, О. В. Ланкин, Д. А. Багаев // Вопросы защиты информации. – 2009. – № 2(85). – С. 8-10.
30. Недопека А. С. Анализ защищённости автоматизированных систем по организации грузоперевозок / А. С. Недопека, К. И. Бушмелева // Национальная Ассоциация Ученых. 2015. – № 10-1(16). – С. 32-35.
31. Авраменко В. С. Модель для количественной оценки защищенности информации от несанкционированного доступа в автоматизированных системах по комплексному показателю / В. С. Авраменко, А. В. Козленко // Труды СПИИРАН. – 2010. – № 2(13). – С. 172-181. – EDN NCNPZV.
32. Язов Ю. К. Информационные риски в условиях применения технологии виртуализации в информационно-телекоммуникационных системах / Ю. К. Язов, В. Н. Сигитов // Информация и безопасность. – 2013. – Т. 16. – № 3. – С. 403-406. – EDN RVMKBN.
33. Методы оценивания защищенности информации в автоматизированных системах от несанкционированного доступа / А. В. Непомнящих, Г. В. Куликов, Ю. В. Соснин, П. А. Нащекин // Вопросы защиты информации. – 2014. – № 1(104). – С. 3-12. – EDN QDNKMA.
34. Никитин А. А. Методический подход к оценке защищенности автоматизированных систем органов внутренних дел на основе требований нормативной документации / А. А. Никитин, И. Г. Дровникова // Общественная безопасность, законность и правопорядок в III тысячелетии. – 2015. – № 1-3. – С. 131-133. – EDN VRBQLD.
35. Соловьев С. В. Информационное обеспечение деятельности по технической защите информации / С. В. Соловьев, Ю. К. Язов // Вопросы кибербезопасности. – 2021. – № 1(41). – С. 69-79. – DOI 10.21681/2311-3456-2021-1-69-79. – EDN AOEUFT.
36. Авсентьев О. С. Обеспечение защиты информации в процессе создания информационной системы объекта информатизации / О. С. Авсентьев, А. Г. Вальде, Ю. В. Конкин // Вестник Воронежского института МВД России. – 2021. – № 3. – С. 36-48. – EDN FJUSGI.

**References:**

1. GOST R 54581-2011 / ISO/IEC TR 15443-1:2005. Information technology. Methods and means of ensuring security. Fundamentals of trust in IT security. Part 1. Overview and basics. 2012; 27.
2. GOST R 54582-2011 / ISO/IEC TR 15443-2:2005. Information technology. Methods and means of ensuring security. Fundamentals of trust in information technology security. Part 2. Methods of trust. 2019; 52 .
3. GOST R 54583-2011 / ISO/IEC TR 15443-3:2007. Information technology. Methods and means of ensuring security. Fundamentals of trust in information technology security. Part 3. Analysis of trust methods. 2011; 54.
4. GOST R 56045-2014 / ISO/IEC TR 27008:2011. Information technology. Methods and means of ensuring security. Recommendations for auditors regarding measures and means of control and management of information security. 2014; 44 .
5. GOST R ISO/IEC 13335-1-2006. Information technology. Methods and means of ensuring security. Part 1. The concept and models of information and telecommunication technology security management. 2006; 23.
6. GOST R ISO 7498-1-99. Information technology. The relationship of open systems. The basic reference model. Part 1. Basic model. 2006; 62.
7. GOST R ISO 7498-2-99. Information technology. The relationship of open systems. The basic reference model. Part 2. Information security architecture. 1999. 39 p .
8. GOST R ISO/IEC TO 13335-5-2006. Information technology. Methods and means of ensuring security. Part 5. Network Security Management Guide. 2006. 33 with
9. GOST R ISO/IEC 15408-1-2012. Information technology. Methods and means of ensuring security. Criteria for assessing the security of information technologies. Part 1. Introduction and general model. 2012. 56 p.
10. GOST R 50739-95. Computer equipment. Protection against unauthorized access to information. General technical requirements. 2006. 10 p.
11. GOST R 50922-2006. Information protection. Basic terms and definitions // Moscow: Federal Agency for Technical Regulation and Metrology. 2006. 12 c.
12. GOST R 51188-98. Information protection. Testing of software for the presence of computer viruses. Model manual. 1998. 8 p.
13. GOST R 51275-2006. Information protection. The object of informatization. Factors affecting information. General provisions. 2006. 11 p.
14. GOST R 51583-2014. Information protection. The procedure for creating automated systems in a protected version. General provisions. 2014. 18 p.
15. GOST R 52069.0-2013. Information protection. The system of standards. The main provisions. 2013. 15 p.
16. GOST R 52447-2005. Information protection. Information security techniques. The nomenclature of quality indicators. 2005. 27 p.
17. GOST R 52448-2005. Information protection. Ensuring the security of telecommunication networks. General provisions. 2005. 19 p.
18. GOST R 52633.0-2006. Information protection. Information security techniques. Requirements for highly reliable biometric

authentication tools. 2006. 24 p.
19. The Law of the Russian Federation of July 21, 1993 N 5485-1 "On state secrets".
20. Federal Law No. 184-FZ of December 27, 2002 "On Technical Regulation".
21. Federal Law No. 126-FZ of July 07, 2003 "On Communications".
22. Federal Law No. 98-FZ of July 29, 2004 "On Trade Secrets".
23. Federal Law No. 160-FZ of December 19, 2005 "On Ratification of the Council of Europe Convention on the Protection of Individuals with Automated Processing of Personal Data".
24. Federal Law No. 149-FZ of July 27, 2006 "On Information, Information Technologies and Information Protection".
25. Federal Law No. 152-FZ of July 27, 2006 "On Personal Data".
26. Federal Law No. 390-FZ of December 28, 2010 "On Security".
27. Federal Law No. 63-FZ of April 06, 2011 "On Electronic Signature".
28. Application of the method of topological transformation of stochastic networks for evaluating the effectiveness of protective equipment / V. V. Baranov, A.M. Kribel, O. S. Lauta, A. P. Nechepurenko. *Actual problems of information security : Proceedings of the Interuniversity Scientific and Practical Conference*, Samara, May 20-24, 2017; Samara: Insoma-Press, 2017; 47-52. – EDN ZAMPAR.
29. Rogozin, E. A. A method for determining a complex indicator of the security of automated systems / E. A. Rogozin, O. V. Lankin, D. A. Bagaev . *Questions of information protection*. 2009; 2(85): 8-10.
30. Nedopeka, A. S. Analysis of the security of automated systems for the organization of cargo transportation / A. S. Neopeka, K. I. Bushmeleva. *National Association of Scientists*. 2015; 10-1(16): 32-35.
31. Avramenko, V. S. A model for quantifying the security of information from unauthorized access in automated systems by a complex indicator / V. S. Avramenko, A.V. Kozlenko. *Proceedings of SPIIRAN*. 2010; 2(13): 172-181.
32. Yazov, Yu. K. Information risks in the conditions of application of virtualization technology in information and telecommunication systems / Yu. K. Yazov, V. N. Sigitov // Information and security. 2013; 16 (3): 403-406.
33. Methods of assessing the security of information in automated systems from unauthorized access / A.V. Nepomnyashchikh, G. V. Kulikov, Yu. V. Sosnin, P. A. Nashchekin. *Questions of information protection*. 2014;1(104):3-12.
34. Nikitin, A. A. Methodological approach to assessing the security of automated systems of internal affairs bodies based on the requirements of regulatory documentation / A. A. Nikitin, I. G. Drovnikova. *Public safety, legality and law and order in the III millennium.* 2015;1-3: 131-133. EDN VRBQLD.
35. Soloviev, S. V. Information support of activities on technical protection of information / S. V. Soloviev, Yu. K. Yazov *Issues of cybersecurity*. 2021;1(41): 69-79. DOI 10.21681/2311-3456-2021-1-69-79. – EDN AOEUFT.
36. Avsentiev, O. S. Ensuring information protection in the process of creating an information system of an informatization object / O. S. Avsentiev, A. G. Valde, Yu. V. Konkin. *Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia*. 2021; 3:36-48. EDN FJUSGI.

**Сведения об авторах:**

Рогозин Евгений Алексеевич, доктор технических наук, профессор, профессор кафедры автоматизированных информационных систем органов внутренних дел; evgenirogozin@yandex.ru

Дровникова Ирина Григорьевна, доктор технических наук, доцент, профессор кафедры автоматизированных информационных систем органов внутренних дел; idrovnikova@mail.ru

Ефимов Алексей Олегович, адъюнкт очной формы обучения; ea.aleksei@yandex.ru

Романова Виктория Романовна, адъюнкт очной формы обучения; romanovna_vika@inbox.ru

**Information about authors:**

Evgeny A. Rogozin, Dr. Sci. (Eng.), Prof., Prof., Department of Automated Information Systems of Internal Affairs Bodies; evgenirogozin@yandex.ru

Irina G. Drovnikova, Dr. Sci. (Eng.), Prof., Assoc. Prof., Department of Automated Information Systems of Internal Affairs Bodies; idrovnikova@mail.ru

Aleksey O. Yefimov, full-time adjunct; ea.aleksei@yandex.ru

Victoria R. Romanova, adjunct of full-time education; romanovna_vika@inbox.ru

**Конфликт интересов/Conflict of interest.**

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

**Поступила в редакцию/Received** 23.09.2022.

**Одобрена после рецензирования/ Reviced** 12.10.2022.

**Принята в печать/Accepted for publication** 12.10.2022.