ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.05
DOI: 10.21822/2073-6185-2022-49-3-61-67 Обзорная статья /Review article

Системы сетевой безопасности

М.А. Ганжур, А.И. Брюховецкий
Донской государственный технический университет,
344002, г. Ростов-на-Дону, пл. Гагарина, 1, Россия

Резюме. Цель. Системы сетевой безопасности являются одним из ключевых игроков в современной деловой жизни. Некоторые сети являются частными, а другие открыты для общего доступа. Независимо от того, является ли ваша сеть частной или общедоступной, она должна иметь надежную защиту и быть надежно защищенной. В этой статье мы обсудим, с чего начинается безопасность сети, опишем общие меры, предпринимаемые для ее безопасности. **Метод.** Исследование определяется необходимостью решения задачи алгоритмического и математического обеспечения оценки функциональной безопасности сети на основе моделирования систем и нахождения ошибочных позиций. **Результат.** Предложено развертывание частной сетевой системы, которая предназначена и обслуживает определенную группу людей для общения, совместной работы и совместного использования. **Вывод.** Предложенные методы могут быть эффективными для защиты сети от атак и других угроз безопасности. Хорошо продуманные корпоративные политики имеют решающее значение для определения и контроля доступа к различным частям сети.

Ключевые слова: сетевая безопасность, информационная безопасность, атаки, риски, угрозы безопасности, вирусы

Для цитирования: М.А. Ганжур, А.И. Брюховецкий. Системы сетевой безопасности. Вестник Дагестанского государственного технического университета. Технические науки. 2022; 49(3):61-67. DOI:10.21822/2073-6185-2022-49-3-61-67

Network security systems

M.A. Ganzhur, A.I. Bryukhovetsky
Don State Technical University,
1 Gagarin Square, Rostov-on-Don 344000, Russia

Abstract. Objective. Network security systems are one of the key players in today's business life. Some networks are private while others are open to the public. Whether your network is private or public, it must be well secured and secure. In this article, we will discuss where network security begins, and describe the general measures taken to secure it. **Method.** The study is determined by the need to solve the problem of algorithmic and mathematical support for assessing the functional security of a network based on system modeling and finding erroneous positions. **Result.** Proposed deployment of a private network system that is designed and serves a specific group of people for communication, collaboration and sharing. **Conclusion.** The proposed methods can be effective in protecting the network from attacks and other security threats. Well-designed corporate policies are critical to defining and controlling access to various parts of the network.

Keywords: network security, information security, attacks, risks, security threats, viruses

For citation: M.A. Ganzhur, A.I. Bryukhovetsky. Network security systems.Herald of the Daghestan State Technical University. Technical Science. 2022; 49 (3): 61-67. DOI: 10.21822 /2073-6185-2022-49-3-61-67

Введение. Безопасность сети — это процесс, который включает в себя все действия, положения и политики, которые организации и системные администраторы предпринимают для защиты целостности и непрерывности операций, коммуникаций, данных и их ценности в своей сети. Чтобы иметь эффективную сетевую безопасность, у должна быть разработана стратегия безопасности.

Постановка задачи. Планирование и разработка такой стратегии является подготовительной частью, которая гарантирует стабильную и целенаправленную безопасность вашей сети; предполагает мониторинг системы, выявление угроз и пути их решения. Хотя обеспечение безопасности сети является сложной задачей, но она может быть обеспечена в этой довольно простой логике. Выявление угроз является одним из ключевых моментов в планировании.

Угрозы для сетей могут иметь различную сущность.

Вирусы и инфекции. Вирусы встречаются в программах, разработанных программистами-мошенниками, и предназначены для самовоспроизведения и заражения систем при запуске определенным событием или службой.

Троянский конь. Программное обеспечение, содержащее трояны, является вредоносным ПО. Трояны кажутся безобидными и даже полезными, но вместо этого они облегчают несанкционированный доступ к системе и изменяют конфигурацию системы или заражают ее. Примерами таких приложений могут быть игры, конвертеры, панели инструментов браузера, гаджеты для рабочего стола, виджеты и т. д. Судя по названию, они всегда кажутся желательными и полезными, поэтому пользователей обманом заставляют скачивать и устанавливать их.

Приложения или апплеты – вандалы. Вандалы – это программные приложения или апплеты, которые наносят ущерб сетям и системам. В отличие от троянских программ, вандалы исключительно стремятся сломать или разрушить систему на «кусочки», не получая доступа к каким-либо данным и не манипулируя ими.

Атаки. Сетевые системы атакуют с разными целями:

– Разведывательные атаки направлены на сбор информации и данных для компрометации сетей;

– Атаки доступа используют уязвимости сети для получения доступа к электронной почте, базам данных и манипулирования данными;

– Атаки типа «отказ в обслуживании», также известные как DoS-атаки, которые блокируют доступ части или всей компьютерной системе. Такие атаки практически невозможно отследить и остановить.

Перехват данных. Перехват данных – это прослушивание сетевых коммуникаций. Перехват также может использоваться не только для перехвата данных, передаваемых по сети, но и для изменения этих пакетов данных.

Неавторизованный доступ и вторжение. Аутентификация пользователя является основным действием для сетевой безопасности. Аутентификация осуществляется в основном с использованием имени пользователя и пароля, которые уникальны для каждого пользователя. Существуют также некоторые другие типы аутентификации, такие как аутентификация с помощью мобильного телефона пользователя, карты банкомата, отпечатков пальцев и т. д. Любой несанкционированный доступ к сети может рассматриваться как вторжение в систему.

Социальная инженерия. Это еще одна форма получения конфиденциальной информации, связанной с сетевой безопасностью, например, выдача себя за сотрудника службы технической поддержки и запрос паролей людей. Спуфинг электронной почты — одно из популярных средств социальной инженерии. Это попытка обманом заставить пользователя сделать оскорбительное заявление или раскрыть конфиденциальную информацию, такую как пароль.

Этот список угроз можно бесконечно расширять и разочаровывать. Если кто-то когда-либо сталкивался с любой из этих угроз (а у вас может быть хотя бы один случай, когда вы все еще являетесь простым пользователем ПК), то ущерб и потери, причиненные вашей небезопасной сети, могут быть действительно ощутимыми и безвозвратными.

Управление рисками. Управление рисками является одним из основных элементов планирования сетевой безопасности. Очень важно понимать риски и уметь с ними справляться. Конечно, риски и их определения различаются для разных организаций и сфер бизнеса. Это зависит от приоритетов безопасности и политики, принятой компанией. Управление рисками для сетевой безопасности – это периодическая деятельность, которая включает в себя анализ сети и мониторинг уязвимостей и угроз.

Брандмауэр. Когда мы говорим о сетевой безопасности, мы сразу же связываем ее с понятием брандмауэра. Брандмауэр похож на «супервизор», обеспечивающего соблюдение политики контроля доступа между двумя подключенными сетями. Как только пользователь аутентифицирован, брандмауэр применяет политики доступа, чтобы установить, какие службы разрешены для использования пользователями. Такие инструменты, как брандмауэры и системы обнаружения вторжений, обеспечивают защиту всех областей сети и обеспечивают безопасное соединение. Сетевые брандмауэры бывают двух типов: программные и аппаратные. Как правило, отдельные ПК-станции используют программное обеспечение брандмауэра, в то время как сети используют выделенные устройства брандмауэра. Устройства брандмауэра предназначены для защиты множества компьютеров, подключенных через сеть. Таким образом, выбор и развертывание оптимального межсетевого экрана для вашей сети имеет большое значение. Однако ни один брандмауэр не может обнаружить или остановить все атаки, поэтому недостаточно установить брандмауэр, а затем игнорировать все другие меры безопасности.

Резервные копии. Даже при эффективной защите ваша система не застрахована от технических и электронных сбоев, часто вызванных аппаратным сбоем. Чтобы предотвратить любые потери или критические повреждения вашей сети, вы должны планировать и осуществлять периодическое резервное копирование данных и журналов передачи. Это поможет легко восстановить ваши данные в случае подобных системных сбоев. Это более чем очевидно лучше жить с резервными копиями, чем терпеть убытки.

Программное обеспечение. Предположим, вы уже определили свои угрозы, настроили политику управления рисками и развернули эффективный брандмауэр для своей сети. Что следующее? Теперь вам нужна система программного обеспечения, которая позволит управлять и централизованно контролировать все текущие меры и действия в вашей сетевой системе. В настоящее время ИТ-рынок богат различным программным обеспечением для сетевых решений, и выбор среди них затруднен.

Для получения оптимального программного решения для вашей сетевой безопасности вы можете сначала рассмотреть такие факторы, как целевое решение, способность обрабатывать объемные данные, возможность создавать различные отчеты о состоянии системы и безопасности, настраиваемость и, конечно же, простота в использовании.

Сегодня многие компании специализируются на обзоре и рейтинге программного обеспечения и приложений, доступных на рынке. Рейтинг определяется такими факторами, как функции, удобство для пользователя, производительность, поддержка, соотношение цены и качества и т. д. Поэтому, если вы заинтересованы в развертывании эффективного программного обеспечения и инструментов для сетевой безопасности, вам следует более внимательно изучить некоторые популярные рейтинги авторитетных рецензентов.

Методы исследования. Пусть данная задача описывается следующими показателями, обладающими двумя управляющими входными, тремя исполнительскими выходами и определённой структурой, отображающей движение и логическое преобразование командной информации. Векторная диаграмма исследуемой структуры приведена на рис. 1.

Входы x1, x2 – и управляющие. Выходы y1, y2, y3 – исполнительские. Узел 5 дизъюнктивного типа «УДТ», а узел 6 – конъюнктивного типа (УКТ). Остальные операторы графа одновходовые, а поэтому выполняют лишь функции преобразования входной информации в её выходную форму.

Предположим, что в структуре может отсутствовать нарушитель (назовем это нулевым состоянием или присутствует, но не более чем один (таких состояний будет 8)).

Синдромы состояний системы можно отобразить наличием (обозначим это 1) или отсутствием (обозначим это 0) командной информации на исполнительских выводах при различных комбинациях управляющих команд на выходах (1 – наличие команды, 0 – отсутствие таковой).

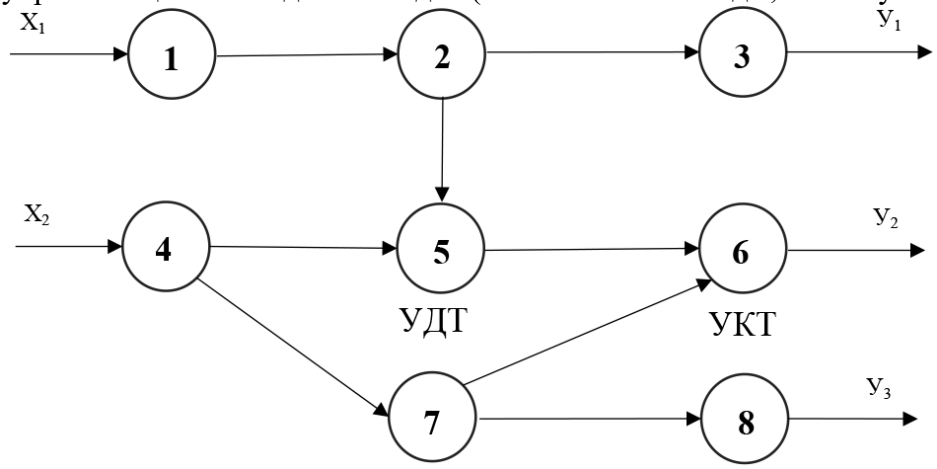

Рис. 1. Векторная диаграмма исследуемой структуры
Fig. 1. Vector diagram of the structure under study

Таблица синдромов приобретает вид (табл.1).

Таблица 1. Таблица синдромов выходов y_1, y_2, y_3
Table 1. Table of output syndromes y_1, y_2, y_3

Состояния входов Input states x1, x2	Нарушитель (номер в структуре) Intruder (number in the structure)								
	0	1	2	3	4	5	6	7	8
00	000	100	100	100	000	000	010	001	001
01	011	111	111	111	000	001	001	000	010
10	100	000	000	000	111	100	110	101	101
11	111	011	011	011	100	101	101	100	110

По таблицам синдромов могут быть построены тестовые последовательности для определения места нарушителя (рис.2). Длина тестовой последовательности может быть разной, а в некоторых случаях она может состоять даже из одного шага. Так нарушитель с номером 6 обнаруживается сразу же при отсутствии входных воздействий и появлении на выходе у3 несанкционированного сигнала.

Считается, что возможна минимизация тестовых проверок, в которых по определенным правилам изменяются состояния входов, а анализируются состояния выходов. Описанная модель является детерминированной, но возможен и вероятностный подход.

Обсуждение результатов. По результатам анализа синдромов можно предположить возможность решения нескольких задач: первая связана с минимизацией количества тестовых проверок для выявления места нарушения то есть в процессе тестирования имеется возможность подавать на выходы любые возможные комбинации и в любой последовательности для рассматриваемого примера комбинация входов «01» выявляет четыре возможных места нарушения за один шаг с другой комбинацией «00» за один шаг выявляется результат «0» (нарушений нет) и в восьмом разряде.

Другая задача может состоять в том, чтобы за единственную тестовую комбинацию входов получить информацию о наличии или нарушения в одном из максимального множества узлов такой комбинацией относится «10», с помощью которой получается информация о возможных нарушениях в пяти узлах.

Еще одной задачей испытаний может быть такая, которая выявляет нарушения без специальных входных воздействий на систему в рассмотренном примере такая задача позволяет проверить лишь шестой узел «00». Если стоит задача минимальных изменений входных воздействий для контроля конкретного узла, то такая задача решается, и ее итог будет зависеть от того, какой контрольный узел подлежит проверке.

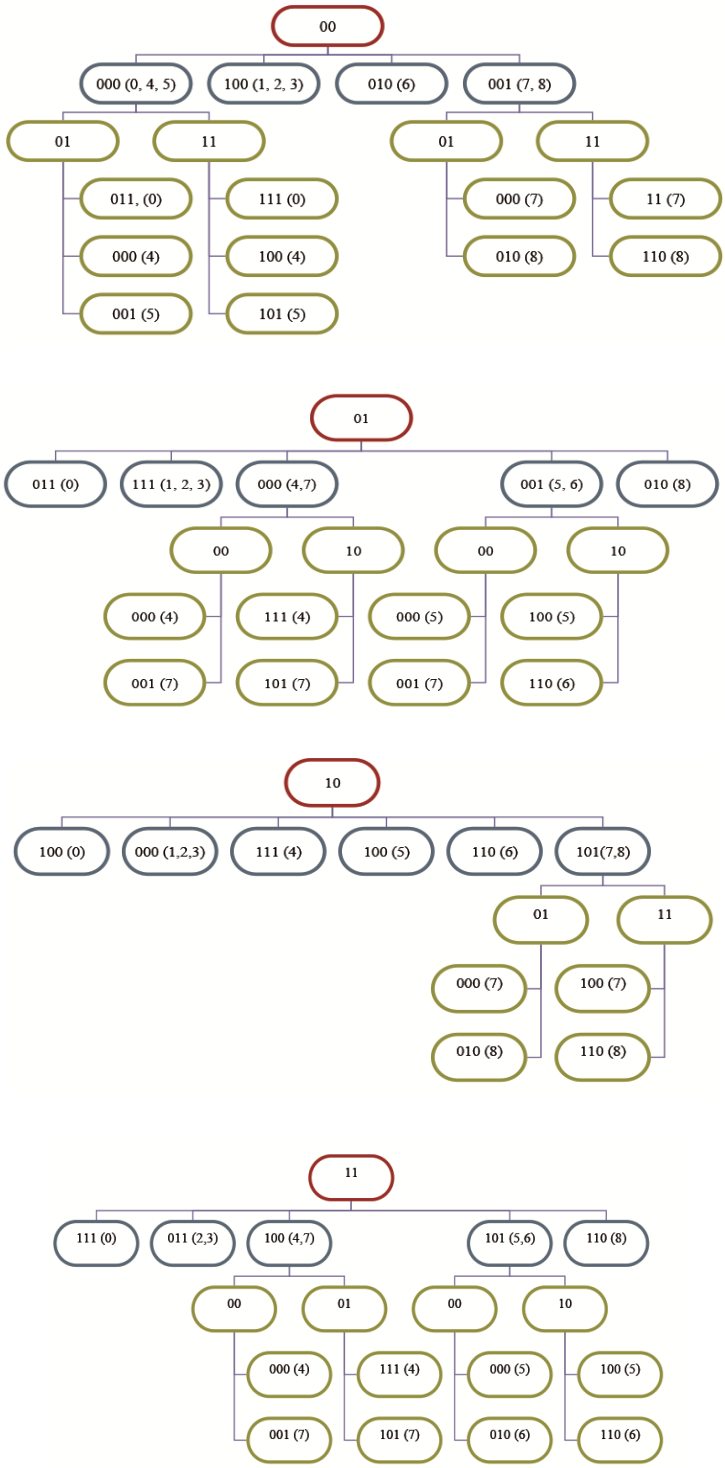

Рис. 2. Деревья-тестограммы
Fig. 2. Testogram trees

В рассмотренном примере для проверки узлов шесть и восемь достаточно изменения тестовых значений лишь на одном входе из двух, а для проверки четвертого и седьмого так же достаточно изменения тестовой информации на одном, но уже другом входе. Если необходимо убедиться в том, что решение задачи достоверно для какого-либо узла, проверки можно проводить так, чтобы исключить знак или в конечном результате в одном или нескольких испытаний.

В рассмотренном примере комбинация «01» с последующей входной комбинацией «00» выделяет в качестве возможного места нарушений четвертого и седьмого узла, а также соответствует состоянию без нарушений. Проводя тестовые комбинации «00» и «11» из множества ноль, четыре и семь выделяется семь, если на входе будет «000», для выделения нулевого или четвертого можно воспользоваться тестовой комбинацией «11» при получении на входе «011», что состояние соответствует исправному нулевому, «100» - нарушение в четвертом узле. Такая задача не является однозначной. Возможны и другие комбинаторные задачи, позволяющие повышать разрешающую способность теста или достоверность окончательного решения.

Вывод. В случае, когда моделируются нарушения, которые носят случайный характер, задача приобретает вероятностный смысл и ее решения возможны лишь с применением соответствующих стохастических подходов. Ни один из этих подходов сам по себе не будет достаточным для защиты сети, но, когда моделируются методы борьбы и идет их объединение, они могут быть очень эффективными для защиты сети от атак и других угроз безопасности. Кроме того, хорошо продуманные корпоративные политики имеют решающее значение для определения и контроля доступа к различным частям сети.

Библиографический список:

1.The Emergence of Virtual Reality and Augmented Reality in the
Security Operations Center / [Электронный ресурс]. Режим доступа: https://securityintelligence.com/the-emergence-of-virtual-reality-and- augmented-reality-in-the-security-operations-center/

2.What is a Security Operations Center (SOC) / [Электронный ресурс]. Режим доступа: https://www.mcafee.com/enterprise/en-us/security- awareness/operations/what-is-soc.html).

3.Новикова Е.С., Модели графического представления информации о защищенности компьютерной сети // Санкт-Петербургский институт информатики и автоматизации РАН. 2013. С. 126-131.

4.Шаньгин В.Ф. Информационная безопасность и защита информации. ДМК-Пресс.2017. С. 254-296) IBM QRadar SIEM / [Электронный ресурс]. Режим доступа: https://www.ibm.com/fi-en/marketplace/ibm-qradar-siem

5.The Future of Augmented Reality and Cybersecurity /[Электронный ресурс]. Режим доступа: https://fedtechmagazine.com/article/2016/03/future-augmented-reality-and- cybersecurity.

6.The Important Difference Between Virtual Reality, Augmented Reality and Mixed Reality / [Электронный ресурс]. Режим доступа: https://www.forbes.com/sites/bernar dmarr/2019/07/19/the-important-difference- between-virtual-reality-augmented-reality-and-mixed-reality/#2155407935d3).

7.Шаньгин В.Ф., Защита информации в компьютерных системах и сетях // ДМК-Пресс .2017. С. 94-120

8. В.А. Фатхи, Н. В. Дьяченко Тестирования безопасности приложений // Инженерный вестник Дона, №5 (2021) URL:http://www.ivdon.ru/uploads/article/pdf/IVD_38__9_Fathi_Dyachenko.pdf_a11917c479.pdf

9. Евсин В.А., Тихонов Н.А., Воробьев С.П. Разработка модуля оптимального размещения информационных ресурсов на узлах вычислительной сети: описание реализуемых методов и структур данных // Инженерный вестник Дона, 2019, №1. URL:ivdon.ru/ru/magazine/archive/n1y2019/5493

10. Берёза Н. В. Современные тенденции развития мирового и российского рынка информационных услуг // Инженерный вестник Дона, 2012, №2. URL: ivdon.ru/magazine/archive/n2y2012/758

11. Зотов А.И., Ганжур М.А., Авакьянц А.В., Характеристика управленческой структуры и системы прохождения команд, Проблемы современного педагогического образования. 2018. № 58-3. С. 111-116

12. Змитрович А.И. Интеллектуальные информационные системы. Мн.: НТООО «ТетраСистемс», 1997. С. 368

13. Фатхи В.А., Фатхи Дм.В., Фатхи Д.В. Функция достижимости и сетевая производная нечеткой сети Петри на основе μ-значной логики // Математические методы в технике и технологиях – ММТТ-19: сб.трудов XIX Междунар. науч. конф.: в 10-и т. Т.6/ под общ. ред. В.С. Балакирева. – Воронеж, Воронеж. гос. технол. акад., 2006. С. 33-37.

14. Ganzhur M.A., Ganzhur A.P., Smirnova O.V. Modeling of critical systems implementing negative events using dual Petri nets. MATEC Web of Conferences Volume 226 (2018), XIV International Scientific-Technical Conference “Dynamic of Technical Systems” (DTS-2018). URL:doi.org/10.1051/matecconf/201822604001

15. Marković N., Živanić J., Lazarević Z., Iričanin B. The Mathematical Model for Analysis and Evaluation of the Transient Process of the three–phase Asynchronous Machine Performance. Serbian journal of electrical engineering (DTS-2018). URL: journal.ftn.kg.ac.rs/Vol_15-3/05-Markovic-ZivanicLazarevicIricanin.pd

16. Гинис Л.А. Развитие инструментария когнитивного моделирования для исследования сложных систем // Инженерный вестник Дона, 2013, №3. URL: ivdon.ru/ru/magazine/archive/n3y2013/1806

17. Гасфилд Д. Строки, деревья и последовательности в алгоритмах: Информатика и вычислительная биология / Пер. с англ. И.В. Романовского. — СПб. Невский Диалект; БХВ-Петербург, 2003. — 654 с.

18. Поликарпова Н.И., Шалыто А.А. Автоматное программирование. - СПб. СПбГПУ, 2008. - 227с.

19. Андреев А.А. Методика выбора базовой архитектуры реконфигурируемой вычислительной системы на основе методов теоретикоигровой оптимизации//Инженерный вестник Дона, 2013, №1. URL: ivdon.ru/magazine/archive/n1y2013/1569

20. Фатхи Дм. В. и др. Бинарные сети Петри с альтернативным маркированием [Текст] // Математические методы в технике и технологиях – ММТТ22: сб. трудов XXII Междунар. науч. конф.: в 10 т. Т. 5. Секция 5 / под общ. ред. В. С. Балакирева. – Псков: изд-во Псков. гос. политехн. ин-та, 2009. – ISBN 978-5-91116-098-9.

References:

1. The Emergence of Virtual Reality and Augmented Reality in the
Security Operations Center / [Electronic resource]. Access Mode: https://securityintelligence.com/the-emergence-of-virtual-reality-and- augmented-reality-in-the-security-operations-center/

2. What is a Security Operations Center (SOC) / [Electronic resource]. Access Mode: https://www.mcafee.com/enterprise/en-us/security-awareness/operations/what-is-soc.html).

3. Novikova E.S., Models of graphical representation of information about the security of a computer network. *St. Petersburg Institute of Informatics and Automation of the Russian Academy of Sciences.* 2013; 126-131. (In Russ)

4. Shangin V.F., Information security and information protection // DMK-Press.2017. pp. 254-296) IBM QRadar SIEM / [Electronic resource]. Access Mode: https://www.ibm.com/fi-en/marketplace/ibm-qradar-siem (In Russ)

5. The Future of Augmented Reality and Cybersecurity / [Electronic resource]. Access mode: https://fedtechmagazine.com/article/2016/03/future-augmented-reality-and-cybersecurity.

6. The Important Difference Between Virtual Reality, Augmented Reality and Mixed Reality / [Electronic resource]. Access mode: https://www.forbes.com/sites/bernar dmarr/2019/07/19/the-important-difference-between-virtual-reality-augmented-reality-and-mixed-reality/#2155407935d3).

7. Shangin V.F., Information security in computer systems and networks. *DMK-Press* .2017; 94-120

8. V.A. Fathi, N. V. Dyachenko Application Security Testing. *Don Engineering Bulletin*, 2021; 5 URL: http://www.ivdon.ru/uploads/article/pdf/IVD_38__9_Fathi_Dyachenko.pdf_a11917c479.pdf (In Russ)

9. Evsin V.A., Tikhonov N.A., Vorobyov S.P. Development of a module for the optimal placement of information resources on the nodes of a computer network: a description of the implemented methods and data structures. *Engineering Bulletin of the Don,* 2019; 1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5493 (In Russ)

10. Bereza N. V. Modern trends in the development of the world and Russian market of information services. *Engineering Bulletin of the Don,* 2012; 2. URL: ivdon.ru/magazine/archive/n2y2012/758 (In Russ)

11. Zotov A.I., Ganzhur M.A., Avakyants A.V., Characteristics of the managerial structure and the command passing system, Problems of modern pedagogical education. 2018;58-3:111-116 (In Russ)

12. Zmitrovich A.I. Intelligent information systems. *Minsk: NTOOO "TetraSystems",* 1997;368

13. Fathi V.A., Fathi Dm.V., Fathi D.V. Reachability function and network derivative of a fuzzy Petri net based on μ-valued logic. Mathematical methods in engineering and technology - MMTT-19: collection of works of the XIX Intern. scientific conf.: in 10 volumes. T.6 / under the general. ed. V.S. Balakirev. - Voronezh, Voronezh. state technol. Acad., 2006; 33-37. (In Russ)

14. Ganzhur M.A., Ganzhur A.P., Smirnova O.V. Modeling of critical systems implementing negative events using dual Petrinets. MATEC Web of Conferences Volume 226 (2018), XIV International Scientific-Technical Conference “Dynamic of Technical Systems” (DTS-2018). URL:doi.org/10.1051/matecconf/201822604001

15. Marković N., Živanić J., Lazarević Z., Iričanin B. The Mathematical Model for Analysis and Evaluation of the Transient Process of the three–phase Asynchronous Machine Performance. Serbian journal of electrical engineering (DTS-2018). URL: journal.ftn.kg.ac.rs/Vol_15-3/05-Markovic-ZivanicLazarevicIricanin.pd

16. Ginis L.A. Development of cognitive modeling tools for the study of complex systems // Engineering Bulletin of the Don, 2013, no. 3. URL: ivdon.ru/ru/magazine/archive/n3y2013/1806 (In Russ)

17. Gasfield D. Lines, trees and sequences in algorithms: Informatics and computational biology / Per. from English. I.V. Romanovsky. *St. Petersburg. Nevsky Dialect; BHV-Petersburg*, 2003; 654. (In Russ)

18. Polikarpova N.I., Shalyto A.A. Automatic programming. *St. Petersburg. SPbGPU,* 2008;227. (In Russ)

19. Andreev A.A. Technique for choosing the basic architecture of a reconfigurable computing system based on game-theoretic optimization methods // Engineering Bulletin of the Don, 2013, No. 1. URL: ivdon.ru/magazine/archive/n1y2013/1569 (In Russ)

20. Fathi Dm. V. et al. Binary Petri nets with alternative labeling [Text] Mathematical methods in engineering and technology - MMTT22: coll. Proceedings of the XXII Intern. scientific conf.: in 10 volumes. Vol. 5. Section 5 / under the general. ed. V. S. Balakireva. Pskov: *Pskov publishing house. state polytechnic in-ta*, 2009. (In Russ)

Сведения об авторах:

Ганжур Марина Александровна, старший преподаватель, кафедра «Вычислительные системы и информационная безопасность»; mganzhur@yandex.ru ORCID 0000-0002-6254-4850

Брюховецкий Андрей Игоревич, магистрант, кафедра «Вычислительные системы и информационная безопасность»; mganzhur@yandex.ru

Information about authors:

Marina A. Ganzhur, Senior Lecturer, Department of Computing Systems and Information Security; mganzhur@yandex.ru ORCID 0000-0002-6254-4850

Andrey I. Bryukhovetsky, Undergraduate, Department of Computing Systems and Information Security; mganzhur@yandex.ru

Конфликт интересов/Conflict of interest.

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

Поступила в редакцию/Received 30.07.2022.

Одобрена после рецензирования/ Reviced 23.08.2022.

Принята в печать/Accepted for publication 23.08.2022.