TASHKENT STATE UNIVERSITY OF ECONOMICS

RAQAMLI IQTISODIYOT VA AXBOROT TEXNOLOGIYALARI

2022

ELEKTRON ILMIY JURNALI MAXSUS SON

РАҚАМЛИ ИҚТИСОДИЁТ ВА АХБОРОТ ТЕХНОЛОГИЯЛАРИ
DIGITAL ECONOMY AND INFORMATION TECHNOLOGY
Илмий электрон журнал | Scientific electronic journal

МУАССИС | FOUNDER
Тошкент давлат иқтисодиёт университети
Tashkent State University of Economics

ТАҲРИР КЕНГАШИ РАИСИ | CHAIRMAN OF THE EDITORIAL BOARD
Шарипов Конгратбой Авезимбетович – т.ф.д., профессор
Sharipov Kongratboy Avezimbetovich – doctor of technical sciences, professor

БОШ МУҲАРРИР | EDITOR-IN-CHIEF
Абдуллаев Мунис Курбонович – и.ф.ф.д. (PhD), доцент
Abdullayev Munis Kurbonovich – PhD, docent

БОШ МУҲАРРИР ЎРИНБОСАРИ | DEPUTY CHIEF EDITOR
Вафоев Бобуржон Расулович – и.ф.н., доцент
Vafoev Boburjon Rasulovich – PhD, docent

МАСЪУЛ КОТИБ | EXECUTIVE SECRETARY
Л.А. Аблазов | Ablazov L.A.

ВЕБ-АДМИНИСТРАТОР | WEBMASTERS:
Н.Я. Нурсаидов, А.Ш. Махмудов | Nursaidov N.Ya., Makhmudov A.Sh.

ТАҲРИРИЯТ АЪЗОЛАРИ | EDITORIAL BOARD

С.С. Гулямов – и.ф.д., академик.
Б.А. Бегалов – и.ф.д., профессор.
М.П. Эшов – и.ф.д., профессор.
О.Қ. Абдурахмонов – и.ф.д., доцент.
К.Б. Ахмеджанов – и.ф.д., профессор.
И.М. Алимардонов – и.ф.д., доцент.
Р.Салиходжаев – и.ф.ф.д. (PhD).
Проф. Холназар Амонов (Чехия).
Проф. Ҳамид Эргашев (Англия).
Проф. Карина Татек Банетти (Чехия).
Проф. Одиложон Абдураззаков (Германия).
Проф. Эко Шри Маргианти (Индонезия).
Проф. Дмитрий Назаров (Россия).
Проф. Н.М. Сурнина (Россия).
Проф. Марк Розенбаум (АҚШ).
PhD. Абдул-Рашид (Афғонистон).
PhD. Аҳмед Мохамед Азиз Исмоил (Миср)
PhD. Бекзод Саидов – (АҚШ).
А.А. Исмаилов – и.ф.д., профессор.
И.Е. Жуковская – и.ф.д. (DSc), профессор.
Т.С.Кучкоров – и.ф.д. (DSc), профессор.
Р.А. Дадабаева – и.ф.н., доцент.
Ш.И. Хашимходжаев – и.ф.н., доцент.
А.А. Абидов – т.ф.н., доцент.
И.М. Абдуллаева – и.ф.н., доцент.
Н.Б. Абдусаломова – и.ф.д. (DSc), профессор.
Р.Х. Насимов – т.ф.н., доцент.
А.Б. Бобожонов – и.ф.ф.д. (PhD).
С.О. Хомидов – и.ф.ф.д. (PhD).
Ш.С. Егамбердиев – и.ф.ф.д. (PhD).

MUNDARIJA:

RAQAMLI IQTISODIYOT VA AXBOROT TEXNOLOGIYALARI KAFEDRASI
RIAT

7. Ўзбекистон Республикаси Президентининг “Рақамли иқтисодиёт ва электрон ҳукуматни кенг жорий этиш чора-тадбирлари тўғрисида”ги ПҚ-4699-сон қарори. 28.04.2020. https://lex.uz/docs/4800657
8. Ўзбекистон Республикаси Президенти Шавкат Мирзиёевнинг Олий Мажлисга Мурожаатномаси. “Халқ сўзи” газетаси № 19 (7521). 2020 йил 25 январь.
9. Ablyazov T., Asaul V. On competitive potential of organization under conditions of new industrial base formation // SHS Web of Conferences. 2018. Vol. 44. 00003.
10. Кощеев В.А., Цветков Ю.А. Цифровая трансформация банковского сектора. https://cyberleninka.ru/article/n/tsifrovaya-transformatsiya-bankovskogo-sektora
11. http://www.cbu.uz/uz/payment-systems/remote-banking-services/
12.https://cbu.uz/upload/medialibrary/ca1/Markaziy_bankning_2021_yil_uchun_hisoboti.pdf

АНАЛИЗ СОВРЕМЕННЫХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Абидов А.А.,
доцент кафедры «Цифровой экономики и информационных технологий»

Мирзаахмедов Д.М.,
старший преподаватель кафедры «Цифровой экономики и информационных технологий»

Аннотация

В статье анализируются внешние и внутренние угрозы информационной безопасности. Ведь для формирования безопасности информационных данных человека, отдельной компании или всего общества требуется иметь представление о возможных угрозах информационной безопасности. Вследствие реализации данных угроз выделяются приоритеты для специалистов в сфере информационных технологий и безопасности.

Калит *с*ўзлар

Информационная безопасность, информационная среда, ИТ-инфраструктура, угрозы, информационные системы.

Введения. Общемировые процессы информационной глобализации диктуют не только необходимость повсеместного внедрения ИКТ в экономике и сферах жизни стран, но и условия обеспечения безопасности информационных систем. Узбекистан одним из первых в Центральной Азии присоединился к международной системе безопасности в сфере информационных и коммуникационных технологий.

В современном мире важнейшими продуктами стали знания и осведомленность, на лидирующие позиции вышла сфера услуг, стремительно развивается глобальное информационное пространство, при этом современные информационные технологии предоставляют не только новые возможности в решении различных проблем, но и создают принципиально новые вызовы и угрозы.

Появление новейших информационных технологий и систем, развитие и расширение функций социальных сетей, внедрение в социальные сети самых различных сервисов и их алгоритмизация создали инструменты превращения исторического процесса развития человечества из неуправляемого в управляемое и даже проектируемое, появились возможности создавать реальность, не соответствующую действительности, осуществлять воздействие на массовое сознание миллионов людей по всему миру.

Появилось понятие «информационная бедность», которое отражает возможности доступа к современным информационным технологиям и информационным ресурсам.

Методология. Государства с развитой информационной средой используют свое доминирующее положение в информационном пространстве для достижения экономических и военно-политических целей. Традиционные средства войны достаточно дороги, тогда как информационные способы воздействия являются прекрасной альтернативой. Спектр воздействий достаточно широк: от дискредитации работы государственных органов до нанесения ударов по критически важной инфраструктуре. Проведение такого комплекса действий приводит к потере управляемости в стране, экономическому спаду, создаются условия для возникновения гражданских конфликтов.

В июле 2016 г. в Варшаве на очередной сессии Совета НАТО киберпространство отнесено к перечню сфер ведения военных действий. На сессии были приняты «Обязательства по обеспечению кибероборонны», предусматривающие финансирование профильных программ, развитие взаимодействия между национальными структурами, активизацию обмена данными о киберугрозах, повышение квалификации сотрудников национальных структур в сфере кибербезопасности, отработку вопросов кибероборонны в ходе мероприятий оперативной и боевой подготовки.

Необходимо отметить, что информационные войны уже ведутся не только государствами, но и корпорациями, и политиками, и религиозными организациями[1]. Основным оружием при этом выступают средства массовой информации.

По мере нарастания объема информации людям становится труднее ориентироваться в ее содержании, ограждать себя от ее избытка и нежелательного контента. Распространение «экранной» культуры, неизбежность столкновения с виртуальной реальностью, в которой трудно различимы иллюзия и действительность, создают проблемы психологического характера.

В настоящее время [3] встроенное программное обеспечение, работающее в критически важных с точки зрения безопасности системах, таких как авионика (бортовое радиоэлектронное оборудование), вычисление миссии и управление автомобилем, в основном используется для сбора информации от внешних раздражителей и своевременно реагировать на различные помехи среды. Например, IEC61508 [4] предлагает набор методов оценки риска.

Метод, основанный на статистике, такой как моделирование Монте-Карло [5], был используемые для работы с переходными неисправностями, зависели от имитационного эксперимента с большими количествами образцов.

Структура отказоустойчивости программного обеспечения в режиме реального времени системы [6] и метод контрольно-пропускного и временного резервирования [7] дают основные модели прогнозирования надежности программного обеспечения. А. Бернс и др. [8] ввел вероятностную модель в анализе расписания в рамках вероятностной гарантии того, что все задачи всегда необходимо завершать к их срокам. И. Бростер и др. [9] расширил этот метод в сети CAN вычислять точные прогнозы вероятности отказа по распределению вероятностей время отклика. Однако эти подходы [8,9] имеют определенные ограничения и приводят к крайне пессимистичным результатам.

Многовариантные программы могут быть реализованы на однопроцессорных, многомашинных, многопроцессорных и других типах систем. Такую избыточность естественно называть неидентичной (она может быть отнесена и к аппаратуре). Подход к многовариантному программированию предложен в [13], такого рода предложения сделаны также в [10, 14, 15, 16], а его современная практически реализуемая форма дана в [11, 12] с использованием термина «многовариантное программирование» (TV-version programming).

Результаты. Можно выделят три главных направления угроз [2].

Первое – искусственный интеллект будет использован для выявления потенциальных жертв, обнаружения уязвимостей программного обеспечения и проведения хакерских атак. Хакерские атаки станут намного масштабнее и эффективнее, при этом искусственный интеллект позволит использовать уязвимости человека. В настоящее время с использованием искусственного интеллекта проводятся работы по созданию реалистичных оригинальных изображений и звуков. Использование таких технологий позволит автомобилям-беспилотникам получать изображения пешеходов и автомобилей в самых разных ситуациях и тренировать себя, не выезжая на улицу. Между тем использование злоумышленниками синтеза речи человека увеличивает вероятность того, что пользователь нажмет на ссылку,

запускающую вирус, или скачает нужное злоумышленникам приложение.

Второе направление – это применение искусственного интеллекта в политической сфере. Политические силы могут использовать искусственный интеллект для манипулирования общественным мнением. Искусственный интеллект может генерировать фейковые новости в таких количествах, что пользователю практически невозможно будет вычленить среди них настоящие. Повысится эффективность и адресность пропаганды. С помощью искусственного интеллекта может быть сделан шаг вперед в изучении основ психологии поведения человека, что также будет использовано для манипулирования поведением человека.

Третье направление – это организация атак на физические объекты. Такие атаки могут быть совершены с использованием массового применения беспилотников или автоматизированных боевых комплексов. Появятся возможности по злонамеренному внедрению в системы беспилотных автомобилей с дальнейшими авариями или нападениями с их участием.

Рост потенциала угроз кибербезопасности ставит задачи найти оптимальные механизмы предотвращения и противодействия современным информационно-технологическим угрозам, что напрямую связано с проблемами науки и образования.

1. Общенаучные проблемы обеспечения информационной безопасности:

– общеметодологические проблемы обеспечения информационной безопасности (проблемы формирования понятийного (терминологического) аппарата в области информационной безопасности;

– проблемы развития нормативного правового и нормативного технического обеспечения информационной безопасности;

– проблемы обеспечения безопасности индивидуального, группового и массового сознания (проблемы обеспечения защищенности личности, общества и государства от деструктивных информационных воздействий;

– проблемы противодействия использованию информационных технологий в преступных целях;

– проблемы сдерживания и предотвращения военных конфликтов, которые могут возникнуть в результате агрессивного и иного враждебного использования информационных технологий.

2. Научно-технические проблемы обеспечения информационной безопасности:

– проблемы развития современных информационных технологий, отечественной индустрии средств информатизации, телекоммуникации и связи (проблемы развития и совершенствования информационной инфраструктуры;

– обеспечения технологической независимости в области создания и использования отечественной электронной компонентной базы и микропрограммного обеспечения, доверенных информационных технологий, вычислительной техники, телекоммуникации и связи; предотвращения возможности включения в информационные технологии скрытых вредоносных функций, снижения опасности их применения);

– проблемы защиты информационных ресурсов, информационных систем и сетей связи;

– проблемы использования информационных технологий в оперативно-разыскной деятельности (выявления и пресечения преступлений, совершенных с использованием информационных технологий; разработки методов и средств и проведения оперативно-разыскных мероприятий в информационных системах и сетях связи).

3. Проблемы кадрового обеспечения информационной безопасности:

– общеметодологические проблемы кадрового обеспечения информационной безопасности и развития содержания профессионального образования в области информационной безопасности;

– проблемы организационного и нормативного правового обеспечения системы подготовки кадров в области информационной безопасности;

– проблемы ресурсного и технологического обеспечения подготовки кадров в области информационной безопасности (разработки концепции материально-технического обеспечения образовательных программ различного уровня в области информационной безопасности и использования комплексов учебно-тренировочных средств и полигонов (компьютерных полигонов) для обеспечения учебного процесса по образовательным программам в области информационной безопасности).

4. Проблемы формирования системы международной информационной безопасности:

– проблемы установления международного правового режима нераспространения «информационного оружия», уменьшения опасности его использования;

– проблемы противодействия использованию информационных и коммуникационных технологий в террористических целях;

– проблемы обеспечения информационной безопасности трансграничных критических информационных инфраструктур, в области противодействия преступности в сфере использования информационных и коммуникационных технологий и др.

Анализ. Расширяются масштабы применения вредоносного программного обеспечения. 2017 г. можно назвать годом применения вирусов-шифровальщиков. В течение всего года осуществлялись масштабные кибератаки на нефтяные, телекоммуникационные, финансовые и логистические компании.

12 мая 2017 г. в Испании нападению с использованием вируса-шифровальщика WannaCry подверглись компьютерные сети крупнейших компаний в сфере телекоммуникаций, газоснабжения и поставок электричества с требованием выкупа. Пользователям предлагалось перевести сумму в биткойнах, эквивалентную 300 долларам США, в течение трех дней по указанному адресу, после чего пользователю на электронную почту будет выслан ключ для разблокировки компьютера. Если выкуп не поступал своевременно, то его сумма автоматически удваивалась. На седьмой день, если WannaCry не был удален с инфицированной системы, зашифрованные файлы уничтожались. Параллельно с шифрованием данных вредоносная программа проводила сканирование адресов локальной сети для последующего заражения новых компьютеров. Всего за три майских дня 2017 г. вирусшифровальщик атаковал 200 000 компьютеров в 150 странах мира. Вирус прошелся по сетям университетов в Китае, заводов Renault во Франции и Nissan в Японии, железнодорожного оператора Deutsche Bahn в Германии. В России атаки были совершены на сети МВД, Мегафона, Сбербанка.

В июне 2017 г. атаки повторились уже с использованием новой модификации вирусашифровальщика Petya. В отличие от WannaCry истинная цель нового вируса заключалась не в получении денежной выгоды, а в нанесении максимального ущерба. Новая версия вируса, получившая название NotPetya, не предполагала возможность расшифровки информации на жестком диске.

27 июня 2017 г. была совершена масштабная атака на нефтяные, телекоммуникационные и финансовые компании России и Украины.

Компьютеры в НПЗ «Башнефти», «Башнефть-Добычи» и управлении «Башнефти» единовременно перезагрузились, после чего скачали неустановленное программное обеспечение и вывели на экран заставку вредоносной программы – вымогателя денежных средств. Только переход на резервную систему управления позволил избежать серьезных последствий.

В ходе атак была атакована крупнейшая логистическая компания A.P. Moller – Maersk. Атака оказалась пагубной для APM Terminals, управляющего работой десятков грузовых портов и контейнерных терминалов. В сутки через них проходит более 100 000 грузовых контейнеров.

Работа ИТ-инфраструктуры была приостановлена, десятки судов вынужденно простаивали на рейде. Компании пришлось передать управление перевозками непосредственно в филиалы, расположенные более чем в 130 странах мира, создать с чистого листа временную службу заказов, а также обновить ИТ-инфраструктуру. Ущерб компании составил около 300 млн долларов.

Сейчас мир столкнулся с новой проблемой – искусственный интеллект. Бесконтрольное распространение технологии искусственного интеллекта (AI) может привести к росту киберпреступности и появлению ее новых форм. В 2017 году 26 экспертами в сфере кибербезопасности из Оксфордского, Кембриджского и Стэнфордского университетов и некоммерческих организаций Electronic Frontier Foundation и OpenAI был опубликован 100-страничный доклад «Преступное использование AI: прогноз, профилактика и предотвращение».

Во исполнения возложенных задач по обеспечению информационной безопасности Министерство по развитию информационных технологий и коммуникаций Республики Узбекистан осуществляет следующие мероприятия:

проведение государственной политики и реализация стратегических приоритетов по созданию условий для совершенствования и дальнейшего развития систем обеспечения информационной безопасности в сетях передачи данных, в телекоммуникационных сетях, в телерадиоэфире и информационных системах;

организация работ и участие в разработке законодательных и нормативных актов по вопросам обеспечения информационной безопасности;

осуществление экспертиз проектов по созданию сетей передачи данных на предмет соответствия требованиям углублённой защиты информационных ресурсов и обеспечению информационной безопасности;

организация регулирования деятельности предприятий телекоммуникаций, операторов и провайдеров сетей передачи данных в области защиты информации и информационной безопасности;

организация научных и маркетинговых исследовательских работ, разработки стандартов и других нормативных документов, мониторинга нормативных документов по обеспечению информационной безопасности;

совершенствование системы обеспечения информационной безопасности в телекоммуникационных сетях, в телерадиоэфире и информационных системах;

разработка единых условий и требований по созданию, внедрению и использованию средств обеспечения информационной безопасности;

систематическое изучение передового зарубежного опыта в области защиты информации и информационной безопасности, его ускоренного внедрения на сетях передачи данных;

разработка и реализация мер по обеспечению информационной безопасности, внедрению современных технологий защиты телекоммуникационных сетей, информационных сетей и информационных ресурсов, включая информационную безопасность в сетях телекоммуникаций, в телерадиоэфире и информационных системах, а также дальнейшее развитие технической инфраструктуры по защите информационных ресурсов;

реализация организационно-технических условий на сетях передачи данных Республики Узбекистан для решения задач по информационной безопасности [17].

Выводы и обсуждения. В настоящее время от специалистов в области информационной безопасности требуются знания и навыки, которые находятся на пересечении самых разных областей знаний: информационные технологии, психология, политология, юриспруденция, криминалистика и др.

Между тем выпускники технических вузов не всегда обладают достаточными знаниями и навыками, позволяющими правильно оценить действия нарушителя информационной безопасности, понять политическую составляющую проблем обеспечения информационной безопасности. Выпускники гуманитарных вузов недостаточно разбираются в специфике угроз информационной безопасности, физической природе возникновения каналов утечки информации. Выходом из сложившейся ситуации может стать использование системы переподготовки и повышения квалификации специалистов по защите информации.

Список литературы

1. Выписка из Основных направлений научных исследований в области обеспечения информационной безопасности Российской Федерации. http://www.scrf.gov.ru/ security/information/ document155/ (дата обращения: 10.04.2018). – Загл. с экрана.
2. Тершуков, Д. А. Об обеспечении международной информационной безопасности / Д. А. Тершуков // Материалы VI Всероссийской научно-практической конференции «Актуальные вопросы информационной безопасности регионов в условиях глобализации информационного пространства», г. Волгоград, 27–28 апреля 2017 г. – Волгоград : Изд-во ВолГУ, 2017. – С. 3–6.
3. Chen X., Hou W., Zhang Y. Reliability Evaluation of Embedded Real–time System based on Error Scenario. From the book Current Trends in Computer Science and Mechanical Automation Vol.2 Published by De Gruyter Open Poland 2022 https://doi.org/10.1515/ 9783110584998-056
4. International Electrotechnical Commission (2010) Functional safety of electrical/electronic/ programmable electronic safety–related systems.
5. M. Sebastian, R. Ernst (2008) Modelling and Designing Reliable On-Chip-Communication Devices in MPSoCs with Real-Time Requirements. In: 13th IEEE International Conference on Emerging Technologies and Factory Automation, pp.1465–1472.
6. T. Anderson, J.C. Knight (1983) A Framework for Software Fault Tolerance in Real-Time Systems. IEEE Transactions on Software Engineering, SE-9(3): 355–364.
7. C. M. Krishna, A. D. Singh (1993) Reliability of Checkpointed real-time systems using time redundancy. IEEE Transactions on Reliability, 42(3): 427–435
8. A. Bums, S. Punnekkat, L. Strigini, D.R. Wright (1999) Probabilistic scheduling guarantees for fault-tolerant real-time systems. In: Dependable Computing for Critical Applications, pp.361-378

9. I. Broster, A. Burns, G. Rodriguez–Navas (2002) Probabilistic analysis of CAN with faults. In: 23rd IEEE Real-Time Systems Symposium, pp 269–278.
10. Avizienis A. Fault-tolerance and fault-intolerance: complementary approaches to reliable computing. - In: Proc. Int. Conf. Reliable Software. Los Angeles, 1975. N. Y. ACM, 1975, p. 458-464.
11. Avizienis A., Chen L. On the implementation of iV-version programming for software fault-tolerance during program execution.– In: Proc. 1977 COMPSAC. Int. Computer Software and Applications Conf. Chicago, 1977. p. 149–155.
12. Chen L., Avizienis A. Aversion programming: a fault-tolerance approach to reliability.
Elmendorf W. R. Fault-tolerant programming.–In: Int. Symp. Fault-Tolerant Computing, 1972, p. 79–83.
13. Fischler M. A., Firschein O., Drew D. L. Distinct software: an approach to reliable computing.– In: Proc. 2nd USA – Japan Computer Conf. Tokyo, 1975, p. 573–579.
14. Girard E., Rault J.-C. A programming technique for software reliability.– In: Proc. IEEE Symp. Computer Software Reliability, 1973. N. Y., 1973, p. 44–50.
15. Kopetz H. Software redundancy in real time systems. - In: Information Processing 74. Proc. IFIP Congr. 74, 1974, v. 2, p. 182–186
16. [https://mitc.uz/ru/pages/info_security]

ОЛИЙ ТАЪЛИМ МУАССАСАЛАРИДА РАҚАМЛИ ТЕХНОЛОГИЯЛАРНИ ҚЎЛЛАШНИНГ ИЛҒОР ХОРИЖИЙ ТАЖРИБАЛАРИ

Абдуллаев Мунис Курбанович,
Тошкент давлат иқтисодиёт университети Рақамли иқтисодиёт ва ахборот технологиялари кафедраси мудири

Зарипов Баҳодир Бобомурод ўғли,
Тошкент давлат иқтисодиёт университети таянч докторанти

Аннотация

Олий таълим муассасаларида рақамли технологияларни жорий қилиш орқали таълим сифати ва илмий тадқиқотлар самарадорлиги ошишини хорижий тажрибалар орқали намоён этишга бағишланган ушбу мақолада Европа мамлакатлари таълим тизимида рақамли технологияларни қўллаган ҳолда эришган ютуқлари таҳлил қилинди. Германия олий таълим тизимида булутли технологиялардан фойдаланиш ҳолати келтириб ўтилди ва таълим соҳасида рақамли технологияларни қўллаш орқали эришилаётган натижалар келтириб ўтилди.

Калит *с*ўзлар

Рақамли технологиялар, булутли технологиялар, интернет, инновациялар, бизнес, самарадорлик.

Кириш. Замонавий дунёда технология инсон ҳаёти, жамият ва бизнес ривожланишига катта таъсир кўрсатади. Технология таълимни ҳам ўзгартиради. Бу билимга бўлган талабни келтириб чиқаради ва ўқитиш ҳамда ўрганишни кенгайтириш орқали кўникма ва билимларни оширади. Таълимда рақамли технологиялардан тобора кўпроқ фойдаланилмоқда. Ўқитишда ва илмий қўллаб-қувватловчи муҳитга эга бўлиш жуда муҳимдир. Кўпгина талабларга жавоб берадиган технология жуда муҳим ва рақамли манбалар талабалар ҳамда тадқиқотчилар учун осон бўлиши керак. Олий таълим талабалари

РАҚАМЛИ ИҚТИСОДИЁТ ВА АХБОРОТ ТЕХНОЛОГИЯЛАРИ
DIGITAL ECONOMY AND INFORMATION TECHNOLOGY
Илмий электрон журнал | Scientific electronic journal

Muharrir:
Yaxshiyev H.T.
Musahhih:
Matxoʻjayev A.O.
Tehnik muharrir:
Kamilova D.D.

Litsenziya AI: № 2537 08.02.2022 y. Bosishga ruxsat etildi: 18.10.2022.
Qogʻoz bichimi: 60x84 1/8. Shartli bosma tabogʻi: 12,75.
Adadi: 50 nusxa. № 19/10-2022-sonli buyurtma.

“IMZO PRINT MEDIA GROUP” XK matbaa boʻlimida chop etildi.
100050, Toshkent sh., Mirzo Ulugʻbek tumani, Mirxosilboy ko'chasi, 55-uy.

TASHKENT STATE UNIVERSITY OF ECONOMICS

RAQAMLI IQTISODIYOT VA AXBOROT TEXNOLOGIYALARI KAFEDRASI
RIAT

+998 71 239-28-94 http://dgeconomy.tsue.uz/
dgeconomy_tdiu@mail.ru, dgeconomy@tsue.uz
100066, Toshkent shahri, Islom Karimov ko'chasi, 49-uy.