ISSN 2181-3187

УДК 004.051.5

СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ГЕТЕРОГЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ МУЛЬТИАГЕНТНОГО ПОДХОДА

Мамадалиев Нурилло Азизиллоевич *– старший преподаватель, специальность: Компьютерный инжиниринг; Ферганский филиал Ташкентского университета информационных технологий имени Мухаммада Ал Хорезми, г. Фергана*

Аннотация*: Работа посвящена актуальной задаче защиты информации в сложных гетерогенных информационных системах. Предлагаются подход и архитектура интеллектуальной системы защиты информации, базирующейся на мультиагентном подходе. Рассматривается ее математическая и функциональная модель, а также методика интеллектуального обнаружения угроз.*

Ключевые слова*: защита информации, мультиагентный подход, обнаружение вторжений, интеллектуальные системы защиты информации.*

INFORMATION SECURITY SYSTEMS FOR HETEROGENEOUS INFORMATION SYSTEMS BASED ON A MULTI-AGENT APPROACH

Abstract*: The paper is devoted to the actual problem of information protection in complex heterogeneous information systems. The approach and architecture of an intelligent information security system based on a multi-agent approach are proposed. Its mathematical and functional model is considered, as well as the method of intelligent threat detection.*

Keywords*: information protection, multi-agent approach, intrusion detection, intelligent information protection systems.*

MULTIAGENTLIY YONDOSHISHGA ASOSLANGAN GETEROGEN AXBOROT TIZIMLARI UCHUN AXBOROTNI HIMOYA QILISh TIZIMI.

Annotatsiya: *Ish murakkab geterojen axborot tizimlarida axborotni himoya qilishning dolzarb masalalariga bag'ishlangan. Ko'p agentli yondashuvga asoslangan intellektual axborotni himoya qilish tizimidagi usul va arxitektura taklif etiladi. Uning matematik va funktsional modeli, shuningdek, tahdidlarni aqlli aniqlash usuli ko'rib chiqiladi.*

ISSN 2181-3187

Kalit so'zlar: *axborotni himoya qilish, ko'p vazifali yondashuv, noqonuniy axborot xujumlarini aniqlash, axborotni himoya qilishning intellektual tizimi.*

Введение

Развитие информационных систем (ИС) в настоящее время характеризуется интенсивным изменением подходов к их проектированию. При этом к настоящему времени большая часть ИС представляет собой *Web*-ресурс, доступ к которому осуществляется посредством глобальной сети *Internet*. Благодаря постоянному положительному тренду развертывания широкополосного доступа к сети *Internet*, в том числе и мобильного, а также интенсивному развитию информационных технологий, с помощью которых создаются разнообразные пользовательские сервисы, нагрузка на ИС может составлять тысячи и даже миллионы одновременных сеансов. Поддержка даже нескольких сотен одновременных сеансов пользователей для информационной системы с развитыми динамическими сервисами в «монолитном» исполнении является крайне трудновыполнимой задачей, а в случае существенно большего количества сеансов – просто невыполнимой. В связи с чем основной вектор развития современных ИС, как правило, лежит в плоскости гетерогенных информационных систем, обладающих свойствами динамического расширения как в контексте предоставляемых сервисов, так и в контексте доступности для увеличивающегося количества пользователей ИС. Ярким примером этого является быстрое развитие различных облачных технологий и предоставляемых ими сервисов (*PaaS*, *IaaS*, *SaaS*).

Одной из наиболее важных проблем функционирования гетерогенных ИС является обеспечение информационной безопасности. Однако в отличие от «монолитных» ИС, для которых за долгие годы их развития появились определенные методики и подходы к проектированию систем защиты информации (СЗИ), для гетерогенных ИС ситуация иная. Методики проектирования СЗИ для гетерогенных ИС, разработанные к настоящему времени, содержат лишь комплексы требований, правил, последовательность и содержание этапов, которые сформулированы на неформальном уровне, т.е. механическое (запрограммированное) их осуществление невозможно в силу высокой сложности самой информационной системы и ее распределенностью по множеству вычислительных узлов.

В такой ситуации невозможно заранее спрогнозировать все возможные атаки на гетерогенную ИС и предусмотреть соответствующие сценарии защиты. Поэтому методы обеспечения информационной безопасности гетерогенных систем могут быть основаны только на использовании мультипрограммных комплексов, способных к планированию поведения в

ISSN 2181-3187

сложных средах. Такие мультипрограммные комплексы должны состоять и множества компонентов защиты, специализирующихся по различным типам решаемых задач (обнаружение угроз, вторжений, аномалий в работе и т.п.), взаимодействовать между собой путем обмена информацией с целью принятия более правильного решения, а также уметь адаптироваться к новым видам атак. Такие мультипрограммные комплексы в различных работах часто называют интеллектуальными СЗИ.

В данной статье рассматривается один из подходов к проектированию интеллектуальных СЗИ, основанный на парадигме мультиагентных систем (МАС) [1 – 4]. Такие системы отличаются от традиционных объектно-ориентированных программных систем тем, что в них, наряду с пассивными сущностями (классы и объекты), существуют и активные сущности – агенты, сообщество которых позволяет решать сложные задачи в условиях неопределенности внешней среды. Обнаружение вторжений и аномалий, а также их предупреждение являются примером таких задач в условиях отсутствия исчерпывающего перечня потенциальных угроз [5, 6, 7, 8, 9, 10, 11, 12, 13].

Объект защиты и постановка задачи

С точки зрения архитектурных принципов понятие гетерогенной информационной системы исходит из теории распределенных вычислительных систем, оно может трактоваться в различных аспектах. Под понятием гетерогенной информационной системы мы будем понимать такие системы, которые функционируют в рамках парадигмы многозвенной клиент-серверной архитектуры. Серверная часть системы представляет собой объединение множества узлов (идентичных и разнородных), которые с помощью соответствующей среды взаимодействия образуют единую информационную среду. Под понятием "узел" будем понимать совокупность технологической платформы используемого программного обеспечения, а также технологий обработки и передачи информации. Клиентская часть такой системы представляет собой интернет-браузер или мобильное приложение (программное обеспечения для мобильного вычислительного устройства, – например, смартфона), реализующее интерфейс пользователя, посредством которого он взаимодействует с информационной средой [14, 15, 16, 17, 18, 19, 20, 21, 22, 23].

В качестве примера архитектуры гетерогенной ИС приведем общую архитектуру информационно-образовательной системы «Электронные курсы ТАТУ ФФ», представленную на рис. 1, которую в дальнейшем будем рассматривать в качестве объекта защиты в вопросе проектирования СЗИ. Заметим, что данная архитектура является сравнительно простым примером

ISSN 2181-3187

гетерогенной ИС, однако на схожих моделях основано большинство таких систем.

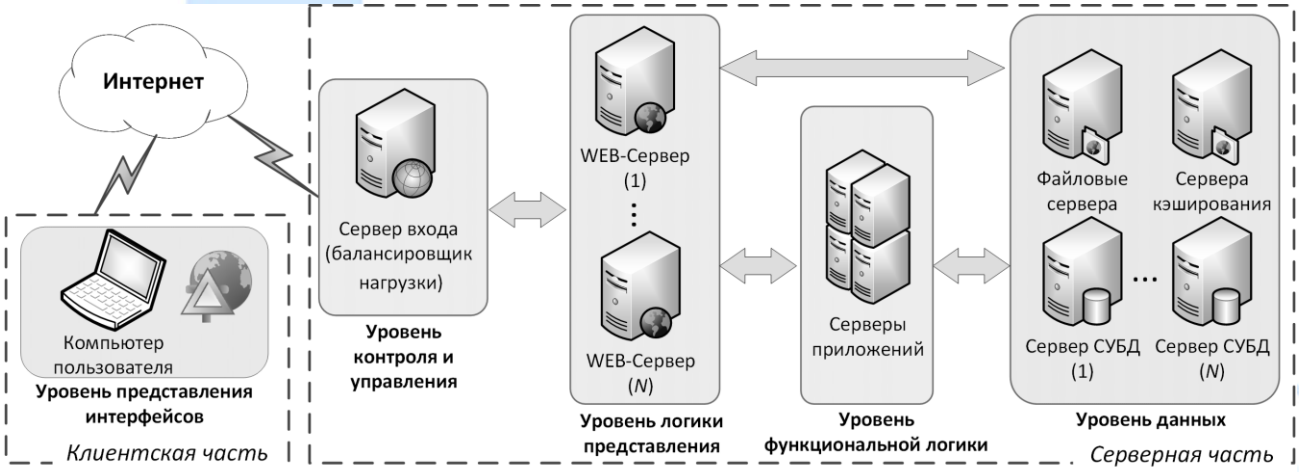

Рис. 1. Пример общей архитектуры гетерогенной ИС.

Структурно модель рассматриваемой гетерогенной ИС (*HIS*) можно описать с помощью теоретико-множественного подхода, – так, ее верхний уровень: $HIS = \{SP, CP\}$, где *SP* и *CP* – серверная и клиентская часть соответственно. Серверная часть $SP = lev_1, lev_2, lev_3, lev_4$ состоит из четырех логических уровней «вертикального» распределения, каждый из которых, в свою очередь, имеет «горизонтальное» распределение на узлы.

С точки зрения аппаратно-технологической архитектуры, каждый узел гетерогенной ИС представляет собой виртуальную машину. Множество всех узлов образует информационно-вычислительный кластер, работающей на некотором множестве физических серверов [24, 25, 26, 27, 28, 29, 30].

Заметим, что в общем случае гетерогенная ИС может иметь вариативное количество логических уровней и узлов. При этом понимается, что при правильном проектировании количество логических уровней в конечном счете определяет функционал ИС, а количество узлов в каждом из них – ее производительность.

Для разработки СЗИ для гетерогенной ИС мы будем исходить из следующих допущений, которые обычно реализуются на практике: все узлы гетерогенной ИС находятся в изолированной сети; доступ из внешней сети есть только к узлам входа; конфигурирование узлов ИС возможно только из изолированной сети; контролирование доступа к изолированной сети осуществляется сторонними системами безопасности (например, посредством *VPN*-шлюза); количество администраторов ИС сильно лимитировано [31, 32, 33, 34, 35, 36, 37, 38, 39, 40].

Разрабатываемая СЗИ должна быть способна: выявлять известные (для

ISSN 2181-3187

СЗИ) виды атак и соответствующие угрозы безопасности на ИС; к эвристическому обнаружению угроз безопасности посредством неизвестных или модифицированных видов атак (для СМИ) на ИС; оповещать администраторов об инцидентах безопасности и аномалиях в работе; самостоятельно принимать решение о предупреждении вторжения в ИС на основе достоверно выявленных вторжениях и собственной базе знаний; к расширяемости по выявлению новых типов угроз и/или атак.

Таким образом, основная задача разработки СЗИ лежит в плоскости перечисленных требований и допущений, а в рамках данной работы заключается в разработке и описании общей архитектуры СЗИ, базирующейся на мультиагентном принципе. При этом следует отметить, что, по существу, разрабатываемая СЗИ представляет собой некоторое гибридное решение, основанное на концепциях систем обнаружения угроз (*IDS*), систем обнаружения аномалий и систем предупреждения вторжений (*IPS*) [41, 42, 43, 44, 45, 46, 47, 48, 49, 50].

Заключение

В данной работе проанализированы современные подходы к созданию адаптивных систем защиты информации для распределенных информационных систем. Данные подходы, несмотря на все их преимущества, в большинстве своем направлены на решение только какой-то конкретной группы задач, комплексно не решая проблему защиты информации в сложных гетерогенных ИС.

В работе представлены проводимые нами исследования на примере архитектуры гетерогенной информационной системы образовательной направленности, которая является действующей и может рассматриваться как объект защиты. В качестве результатов исследований нами изложена концепция адаптивной системы защиты информации, архитектурно базирующаяся на мультиагентном подходе и ориентированная на гетерогенные ИС. Кроме того, в работе отражены общие положения методики обнаружения угроз агентами, в основе которых лежат методы интеллектуального анализа данных и методы машинного обучения.

С практической точки зрения, полученные результаты могут быть полезны разработчикам интеллектуальных систем защиты информации.

ISSN 2181-3187

Используемая литература:

1. *Рассел Стюарт, Норвиг Питер.* Искусственный интеллект: современный подход. – Изд. 2-е / пер. с англ. – М.: Изд. дом «Вильямс», 2006.
2. *Shoham Y., Leyton-Brown K.* Multiagent systems: Algorithmic, Game-Theoretic, and Logical Foundations. – Cambridge University Press, 2009.
3. *Городецкий В.И.* Многоагентные системы: современное состояние исследований и перспек- тивы применения// Новости искусственного интеллекта. – 1996. – №1. – С.44-59.
4. *Городецкий В.И.* Многоагентные системы: основные свойства и модели координации пове- дения // Информационные технологии и вычислительные системы. – 1998. – №1. – С.22-34.
5. *Wooldridge M., Jennings N.* Towards a Theory of Cooperative Problem Solving // (MAA- MAW'94, Odense, Danemark) / Ed. by Y.Demazeau, J.-P.Muller and J.Perram, 1994.
6. *Wooldridge M., Jennings N.* Agent Theories, Architectures and Languages: a Survey // Intelligent Agents: ECAI-94 Workshop on Agent Theories, Architectures and Languages (Amsterdam, The Netherlands, August 8-9, 1994) / Ed. by M.Wooldridge, N.Jennings. – Berlin: Springer Verlag. – 1995. – P.1-22.
7. *Wooldridge M., Jennings N.* Intelligent Agents: Theory and Practice // The Knowledge Engineer- ing Review. – 1995. – Vol.10, №2. – P.115-152.
8. A. Хакимов. МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ ВНЕДРЕНИЯ ERPСИСТЕМ АВТОМАТИЗАЦИИ НА ПРЕДПРИЯТИИ// TATU FF Respublika ilmiy-texnika anjumani -2022 //c- 525-529
9. A. Xakimov SANOAT KORXONALARINING MA'LUMOTLAR BAZALARINI QAYTA ISHLASH TEXNOLOGIK JARAYONLARINI AVTOMATLASHTIRISH// TDTU Respublika miqiyosidagi ilmiy-texnika anjumani// 2021 C-128-129 "
10. Обухов В.А., Горовик А.А., Исследование архитектур и принципов работы современных процессоров / Республиканская научно-техническая конференция по теме «Современные проблемы и решения информационно-коммуникационных технологий и телекоммуникаций». 16-17 апреля 2021 г., ТУИТ ФФ. г. Фергана – с. 217-219.
11. Халилов Д.А., Кушматов О.Э., Обухов В.А., 5 параметров линейки процессоров INTEL: серии, поколения, номера и версии в названии / Республиканская научно-практическая конференция по теме: "Проблемы применения современных информационных, коммуникационных технологий и IT-образования". 24-25 ноября 2021 г., ТУИТ СФ. г. Самарканд – с. 101-105.
12. Обухов В.А. ТУИТ ФФ имени Мухаммада Аль-Хорезми. Диссертационная выпускная работа на тему: "Исследование современных архитектур

ISSN 2181-3187

компьютерных процессоров и разработка компьютерной программы моделирующей работу вычислительных и управляющих узлов процессора". 2022 г.

13. Мохигул А., Мохинур А. ПОНЯТИЕ BIG DATA И ЕГО ОСНОВНЫЕ ХАРАКТЕРИСТИКИ //INTERNATIONAL CONFERENCES ON LEARNING AND TEACHING. – 2022. – Т. 1. – №. 1.
14. Шипулин Ю. Г., Абдуллаев Т. М. Состояние и развитие интеллектуальных оптоэлектронных преобразователей перемещений на основе волоконных и полых световодов //Universum: технические науки. – 2020. – №. 5-1 (74). – С. 5-9.
15. Shipulin Y. et al. Intelligent microprocessor system for control and control of microclimate parameters in vegetable storages using temperature calibrators //Technical science and innovation. – 2021. – Т. 2021. – №. 4. – С. 144-152.
16. Шипулин, Ю. Г., Рустамов, Э., Абдуллаев, Т. М., & Мейлиев, С. Н. (2019). ИНТЕЛЛЕКТУАЛЬНЫЙ ОПТОЭЛЕКТРОННЫЙ ДАТЧИК ТЕМПЕРАТУРЫ С ВОЛОКОННО-ОПТИЧЕСКИМИ ЭЛЕМЕНТАМИ. In Проблемы получения, обработки и передачи измерительной информации (pp. 248-253).
17. Shipulin Y. et al. APPLICATION OF METHODS OF INTERMITTENT VENTILATION OF INDUSTRIAL PREMISES USING A DIGITAL DATA TRANSMISSION SYSTEM //Chemical Technology, Control and Management. – 2021. – Т. 2021. – №. 4. – С. 12-18.
18. Siddikov I. K., Porubay O. V. Neuro-fuzzy system for regulating the processes of power flows in electric power facilities //AIP Conference Proceedings. – AIP Publishing LLC, 2022. – Т. 2432. – №. 1. – С. 020010.
19. Siddikov I., Porubay O. Neural network model of decision making in electric power facilities under conditions of uncertainty //E3S Web of Conferences. – EDP Sciences, 2021. – Т. 304.
20. Сиддиков И. Х., Порубай О. В. ПРИНЯТИЕ РЕШЕНИЙ В УСЛОВИЯХ ОПРЕДЕЛЕННОСТИ И РИСКА НА ОСНОВЕ СТРОГИХ МЕТОДОВ //СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ ФУНДАМЕНТАЛЬНЫХ И ПРИКЛАДНЫХ НАУК. – 2021. – С. 208-214.
21. Порубай О. В., Амиров А. Р. ПРОБЛЕМЫ ПРИНЯТИЯ РЕШЕНИЙ В УСЛОВИЯХ ОПРЕДЕЛЕННОСТИ И РИСКА НА ОСНОВЕ СТРОГИХ МЕТОДОВ //Universum: технические науки. – 2021. – №. 6-1. – С. 32-33.
22. Khonturaev, Sardorbek, and Shohida Eshmatova. "Saving environment using Internet of Things: challenges and the possibilities." Современные образовательные технологии в мировом учебно-воспитательном пространстве 8 (2016): 152-157.

23. А. Хакимов МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ ВНЕДРЕНИЯ ERPСИСТЕМ АВТОМАТИЗАЦИИ НА ПРЕДПРИЯТИИ// TATU FF Respublika ilmiy-texnika anjumani -2022 //c- 525-529
24. A. Xakimov SANOAT KORXONALARINING MA'LUMOTLAR BAZALARINI QAYTA ISHLASH TEXNOLOGIK JARAYONLARINI AVTOMATLASHTIRISH// TDTU Respublika miqiyosidagi ilmiy-texnika anjumani// 2021 C-128-129 "
25. Xamidov E. X. MODELS OF OBJECT DETECTION SYSTEM IN VIDEO STREAMS ON A MOBILE DEVICE //Eurasian Journal of Mathematical Theory and Computer Sciences. – 2022. – Т. 2. – №. 3. – С. 21-26.
26. Khamidovich X. E., Murodovich X. J. Parallel Programming in Java for Mobile App Development //International Journal of Innovative Analyses and Emerging Technology. – 2022. – Т. 2. – №. 3. – С. 69-74.
27. Khamidovich X. E., Murodovichelnur X. J. Computer-Vision Based Method for Human Action Recognition //International Journal of Innovative Analyses and Emerging Technology. – 2022. – Т. 2. – №. 3. – С. 44-47.
28. Khamidovich X. E., Murodovich X. J. Parallel Programming in Java for Mobile App Development //International Journal of Innovative Analyses and Emerging Technology. – 2022. – Т. 2. – №. 3. – С. 69-74.
29. Khoitkulov, A. A., & Pulatov, G. G. (2022). DEVELOPMENT OF ORGANIZATIONAL AND ECONOMIC MECHANISMS TO INCREASE THE CAPACITY OF TEXTILE ENTERPRISES. Gospodarka i Innowacje., 23, 142-145.
30. Khoitkulov A. A. Improving Organizational And Economic Mechanisms To Increase The Power Of Textile Enterprises.
31. M.SobirovTa'limda jarayonida LMS tizimlar taxlili// Analytical Journal of Education and Development -2022 //c- 118-122
32. M.Sobirov Advantages of using LMS as a System for Monitoring, Evaluating and Monitoring Learning Outcomes// International Journal of Development and Public Policy// 2022 C-123-128
33. Xamidov Elnur Khamidovich, Xodjimatov Jahongir Murodovich, 2022/4/2, International Journal of Innovative Analyses and Emerging Technology, 69-74
34. Xamidov Elnur Khamidovich, Xodjimatov Jahongir Murodovichelnur, 2022/4/1, International Journal of Innovative Analyses and Emerging Technology, 44-47
35. EX Xamidov, 2022/3/24, Eurasian Journal of Mathematical Theory and Computer Sciences, 21-26
36. Эльнур Хамидович Хамидов, 2020, Молодой ученый, 37, 8-11
37. O.I.Ergashev & B.A.Mirzakarimov. Портфолио тизимининг тадқиқоти // Central Eurasian Studies Society INTERNATIONAL SCIENTIFIC ONLINE

CONFERENCE ON INNOVATION IN THE MODERN EDUCATION SYSTEM colletions of scientific works Washington, USA - 2021. Part 13 – №. 3. – С. 399-401.

38. O.I.Ergashev & H.Zaynidinov & I.E.Shokirov. Кундалик ҳаётда сунъий интеллектнинг энг яхши 4 та мисоли // Фарғона политехника институтида “Ўзбекистонда ер ресурсларини бошқариш ва улардан фойдаланиш тамойиллари: муаммо ва ечимлар” мавзусида ўтказиладиган Республика онлайн илмий-амалий конференсия 2022, 23-24 сентябрь II-том
39. N.Mamadaliyev-“Linear differential pursuit games with integral constraints in the presence of delay” //Jurnal-Mathematical Notes 2020, 91(5) c.704-713.
40. POLISH SCIENCE JOURNAL – 2021 may, ISSUE 5(38) Part 2
41. Kodirov, E., Turgunov, B., & Muxammadjonov, X. (2019). IN THE WORLD REFUSES TO USE FACE RECOGNITION TECHNOLOGY. Мировая наука, (9), 34-36.
42. Turgunov, B., Komilov, A., Abdurasulova, D., & Umarov, X. (2018). SECURITY OF A SMART HOME. In Перспективные информационные технологии (ПИТ 2018) (pp. 253-256).
43. Тургунов, Б. А., & Халилов, М. М. (2018). СОВРЕМЕННЫЕ СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИОННОГО СИГНАЛА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ОПТИЧЕСКИХ СЕТЯХ. In САПР и моделирование в современной электронике (pp. 195-197).
44. Абдурахмонов, С. М., Кулдашов, О. Х., Тожибоев, И. Т., & Тургунов, Б. Х. (2019). Оптоэлектронный двухволновый метод для дистанционного контроля содержания метана в атмосфере. Письма в Журнал технической физики, 45(4), 11-12.
45. Тохиров, Р., Тургунов, Б., & Мухаммаджонов, Х. (2019). СТРУКТУРНАЯ СХЕМА БЛОКА РАСПОЗНАВАНИЯ РЕЧИ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ УПРАВЛЕНИЯ. Форум молодых ученых, (7), 322-324.
46. Тургунов, Б., Комилов, А., Абдурасулова, Д., & Асроров, С. (2018). Применение беспроводных сетевых технологий в медицинских измерительных системах.
47. Тургунов, Б., Комилов, А., Абдурасулова, Д., & Асроров, С. (2018). ПРИМЕНЕНИЕ БЕСПРОВОДНЫХ СЕТЕВЫХ ТЕХНОЛОГИЙ В МЕДИЦИНСКИХ ИЗМЕРИТЕЛЬНЫХ СИСТЕМАХ. In Перспективные информационные технологии (ПИТ 2018) (pp. 750-755).
48. Тургунов, Б. А., & Халилов, М. М. (2018). РОЛЬ ВОЛОКОННОЙ ОПТИКИ В СЕТЯХ ПОМЕЩЕНИЙ. In САПР и моделирование в современной электронике (pp. 83-86).

ISSN 2181-3187

49. M.Sobirov //Monitoring tizimini avtomatlashtirish jarayoni//Zamonaviy dunyoda ijtimoiy fanlar: nazariy va amaliy zlanishlar//c-2022-115-117
50. O.I.Ergashev & B.A.Mirzakarimov & I.E.Shokirov. Таълим муассасаларида автоматлаштирилган тизимларни асосий ташкил этувчилари // Муҳаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университети Фарғона филиали, “Ахборот-коммуникация технологиялари ва телекоммуникацияларнинг замонавий муаммолари ва ечимлари” Республика илмий-техник анжуманининг маърузалар тўплами. 2019, 30-31 май, III қисм