ӘОЖ 004.4

АҚПАРАТТЫҚ ЖҮЙЕЛЕРДІ ҚОРҒАУДЫҢ ЗАМАНАУИ ӘДІСТЕРІ

Наби А.С.
магистрант, Абай атындағы Қазақ ұлттық педагогикалық университеті, Қазақстан Республикасы

Ғылыми жетекші: Н.А.Курмангалиева
PhD, аға оқытушы, Абай атындағы Қазақ ұлттық педагогикалық университеті, Қазақстан Республикасы

Қазіргі уақытта ақпараттық жүйелердің қауіпсіздігі мен қорғалуы кез келген ұйым үшін маңызды мәселеге айналды. Ақпараттық жүйелерді қорғаудың заманауи әдістері деректердің қауіпсіздігін қамтамасыз ету және жүйелердің сыртқы шабуылдарға қарсы тұру қабілетін арттыру үшін әртүрлі құралдар мен технологияларды қолдануды талап етеді. Бұл мақалада ақпараттық жүйелердің қауіпсіздігін қамтамасыз ету үшін қолданылатын негізгі заманауи әдістер талқыланады. Оларға криптографиялық әдістер, көпфакторлы аутентификация, зиянды бағдарламалардан қорғау жүйелері, желілік қауіпсіздік құралдары және қауіп-қатерлерді анықтау мен алдын алу жүйелері жатады. Сонымен қатар, мәліметтерді қорғаудың жаңа тәсілдері мен ақпараттық жүйелердің қауіпсіздігін арттыру үшін қолданылатын инновациялық технологиялар қарастырылады. Ақпараттық жүйелердің қорғалуының тиімді әдістерін қолдану ұйымдардың ақпараттық қауіпсіздігін қамтамасыз етуге, кибершабуылдар мен деректердің жоғалуы сияқты тәуекелдерді азайтуға мүмкіндік береді. Әсіресе, жаңа технологиялардың енгізілуі мен осы саладағы даму үрдістері ақпараттық қауіпсіздіктің тиімділігін арттыруға зор үлес қосуда. Мақалада қарастырылған әдістер мен шешімдер ақпараттық жүйелердің қауіпсіздігін арттырудағы өзекті мәселелер мен келешектегі даму бағыттарын көрсетеді.

Кілттік сөздер: ақпараттық жүйелер, криптография, көпфакторлы аутентификация, желілік қауіпсіздік, кибершабуылдар, инновациялық технологиялар.

Кіріспе:

Қазіргі заманда ақпараттық жүйелер күнделікті өмірде маңызды рөл атқарады, ал олардың қауіпсіздігі мен қорғалуы кез келген ұйым үшін басты мәселе болып табылады. Жаһандық цифрландыру мен интернеттің дамуымен ақпараттық жүйелерге бағытталған қауіптер де артуда. Бұл жағдай деректердің

сақталуы мен қорғауына қойылатын талаптарды күшейтуде. Ақпараттық жүйелерді қорғаудың заманауи әдістері жаңа технологиялар мен құралдарды пайдалану арқылы жүйелерді сыртқы және ішкі қауіптерден қорғауды қамтамасыз етеді. Осы тұрғыда криптография, көпфакторлы аутентификация, зиянды бағдарламалардан қорғану, және желілік қауіпсіздік сияқты әдістер айтарлықтай маңызға ие. Ақпараттық қауіпсіздік саласындағы үздік тәжірибелер мен инновациялық шешімдер ұйымдардың деректерін қорғап, кибершабуылдарға төтеп беруге көмектеседі. Бұл мақалада ақпараттық жүйелердің қауіпсіздігін қамтамасыз ету үшін қолданылатын негізгі әдістер мен тәсілдер, олардың тиімділігі және даму тенденциялары қарастырылады.

Әдебиеттерге шолу

Ақпараттық жүйелердің қауіпсіздігін қамтамасыз ету қазіргі уақытта ұйымдардың тиімді жұмыс істеуі үшін өте маңызды болып табылады. Ақпараттық жүйелерді қорғау үшін әртүрлі заманауи әдістер мен технологиялар қолданылады. Бұл әдістердің ішінде криптография, зиянды бағдарламалардан қорғау, желілік қауіпсіздік, көпфакторлы аутентификация және қауіп-қатерлерді анықтау жүйелері сияқты маңызды құралдар бар.

Криптографиялық әдістер — ақпаратты қорғаудың негізгі тәсілдерінің бірі болып табылады. Бұл әдіс ақпаратты кодтау және шифрлау арқылы оны заңсыз қол жеткізуден қорғайды. Криптографиялық алгоритмдер, әсіресе AES (Advanced Encryption Standard), қазіргі уақытта ең кең таралған шифрлау әдістері болып табылады. Белявский (2021) криптографиялық әдістердің қауіпсіздік саласындағы рөлін қарастырып, олардың ақпараттық жүйелерді қорғаудағы маңыздылығын атап өткен [4].

Зиянды бағдарламалардан қорғау да ақпараттық жүйелердің қауіпсіздігін қамтамасыз етуде маңызды рөл атқарады. Зиянды бағдарламалар мен вирустар жүйелерді бұзып, ақпаратты ұрлауға немесе бүлдіруге бағытталған. Касперский (2020) зиянды бағдарламаларға қарсы күрес әдістері мен антивирус жүйелерінің тиімділігін зерттеген [5]. Ол антивирус бағдарламалары мен зиянды бағдарламаларды анықтаудың жаңа әдістері туралы мәліметтер келтірген.

Желілік қауіпсіздік — сыртқы шабуылдардан қорғаудың басты шарасы болып табылады. Желілерге қосылған ақпараттық жүйелердің қауіпсіздігін қамтамасыз ету үшін брандмауэрлер, IDS/IPS жүйелері, VPN сияқты құралдар пайдаланылады. Ли мен Чен (2018) желілік қауіпсіздікті қамтамасыз ету үшін қолданылатын заманауи құралдарды талдап, олардың тиімділігін зерттеген [6]. Бұл зерттеулер желілік қорғаныс әдістерінің маңызды аспектілерін көрсетеді.

Көпфакторлы аутентификация жүйелерінің көмегімен жүйеге қол жеткізу үшін тек құпиясөз ғана емес, сонымен қатар қосымша қауіпсіздік факторлары қолданылады. Хіе және Wu (2019) көпфакторлы аутентификацияның жүйелердегі қауіпсіздікті арттырудағы рөлін зерттеп, оның ақпараттық қауіпсіздік саласындағы маңыздылығын көрсеткен [7]. Қауіп-қатерлерді

анықтау және алдын алу жүйелері (IDS/IPS) ақпараттық жүйелердегі аномалияларды анықтап, шабуылдарды ерте кезеңде болдырмауға көмектеседі. Кавва мен Лехал (2021) осы жүйелердің тиімділігін талдап, олардың ақпараттық жүйелерді қорғаудағы рөлін көрсеткен [8]. Олар қауіп-қатерлерді анықтау мен алдын алу бойынша заманауи әдістерді қарастырады.

Ақпараттық жүйелердің қауіпсіздігін қамтамасыз ету үшін жасанды интеллект (AI) және машиналық оқыту (ML) технологиялары да кеңінен қолданыла бастады. Liu және Zhang (2020) жасанды интеллекттің қауіп-қатерлерді анықтау және алдын алу жүйелеріндегі рөлін зерттеп, бұл технологиялардың ақпараттық жүйелерді қорғаудағы тиімділігін талдаған [9]. Қорытындылай келе, ақпараттық жүйелерді қорғаудың заманауи әдістері жүйелердің қауіпсіздігін қамтамасыз ету үшін тиімді құралдар мен әдістерді қамтиды. Криптография, зиянды бағдарламалардан қорғау, желілік қауіпсіздік, көпфакторлы аутентификация және қауіп-қатерлерді анықтау әдістері ұйымдарға қауіпсіздік деңгейін арттыруға және кибершабуылдарды болдырмауға көмектеседі.

Зерттеу әдісі

Зерттеуде сипаттамалық сапалық әдістер қолданылды. Алынған деректерге талдау жасалды. Ақпараттық жүйелерді қорғаудың заманауи әдістері туралы түсінік қалыптастыру мақсатында, мамандар мен студенттерден онлайн сауалнама алынды. Сауалнама Google Forms платформасы арқылы жүргізілді. Сауалнама 10 сұрақтан тұрды. Зерттеуге барлығы 10 ақпараттық қауіпсіздік саласының маманы, 5 университет оқытушысы және 30 ақпараттық жүйелер студенті қатысты. Қатысушылардың жасы 20-45 аралығында болды. Сауалнамада ақпараттық жүйелерді қорғаудың заманауи әдістері мен олардың тиімділігін бағалауға бағытталған сұрақтар қойылды. Сауалнама ашық түрде жүргізілді және барлық қатысушылардың деректері ашық түрде ұсынылды. Тестті әзірлеу кезінде заманауи әдістердің қолданылу ауқымы мен практикалық қолданылу деңгейі ескерілді. Сауалнама алынбас бұрын бірнеше тексерістен өтіп, сараптамадан өтті. Зерттеудің мақсаты ақпараттық жүйелерді қорғаудың заманауи әдістерінің тиімділігін анықтау және оларды болашақ мамандардың оқыту процесінде қолдану қажеттілігін көрсету.

Зерттеу нәтижесі

Мамандар нәтижесі

Мамандардың басым көпшілігі ақпараттық жүйелерді қорғаудың заманауи әдістерінен хабардар екендіктерін және оларды қазіргі заманғы қауіпсіздік жүйелерінде қолданудың маңыздылығын атап өтті. Сонымен қатар, мамандардың (30%) пікірінше, ақпараттық жүйелерді қорғау саласындағы заманауи әдістер тиімді және оларды тұрақты түрде жетілдіріп отыру қажет. Жауап берген мамандардың (50%) ойынша, қазіргі заманғы әдістердің қолданылуы ақпараттық жүйелердің қауіпсіздігін арттырып, түрлі

кибершабуылдарға қарсы тұруға мүмкіндік береді және бұл әдістерді тәжірибеде пайдалануға тырысады . Ал (20%) мамандар бұрынғы әдістерді тиімді деп санайды және жаңа әдістердің енгізілуіне қарсы көзқарас білдірді. Төменде 1-суретте мамандардың ойын диаграмма түрінде көрсеттім:

1- сурет. Мамандардың ойы диаграмма түрінде

Оқытушылар нәтижесі

Оқытушылардың пікірінше, ақпараттық жүйелерді қорғаудың заманауи әдістері болашақ мамандарды оқыту үшін өте маңызды және осы әдістерді оқу жоспарына енгізу қажеттілігі туралы айтты. Оқытушылардың (60%) бұл әдістерді студенттерге үйретуде тиімді деп санайды, ал (18%) оқытушылар қазіргі уақытта жаңа әдістерді жеткілікті деңгейде қолдана алмайтынын көрсетті. Сонымен қатар, (19%) оқытушылар өз сабағында ақпараттық жүйелерді қорғаудың заманауи әдістерін пайдалануға тырысатынын, ал қалғандары (3%) бұл әдістерді көбінесе теориялық түрде түсіндіретіндігін айтты. . Төменде 2-суретте оқытушылардың ойын диаграмма түрінде көрсеттім:

2- сурет. Оқытушылардың ойы диаграмма түрінде

Студенттер нәтижесі

Студенттердің жауаптарына қарағанда, олар ақпараттық жүйелерді қорғаудың заманауи әдістерін өз оқу барысында үйренуге қызығушылық танытады. (65%) студент қазіргі әдістердің тиімділігі мен олардың практикалық қолданылуын бағалауда оң пікір білдірді, ал (35%) студенттер жаңа әдістердің күрделілігіне қатысты алаңдаушылықтарын білдірді. Жауап берген студенттердің пікірінше, заманауи әдістер тек теориялық тұрғыдан ғана емес, практикалық тұрғыдан да үйретілуі тиіс. . Төменде 3- суретте студенттердің ойын диаграмма түрінде көрсеттім:

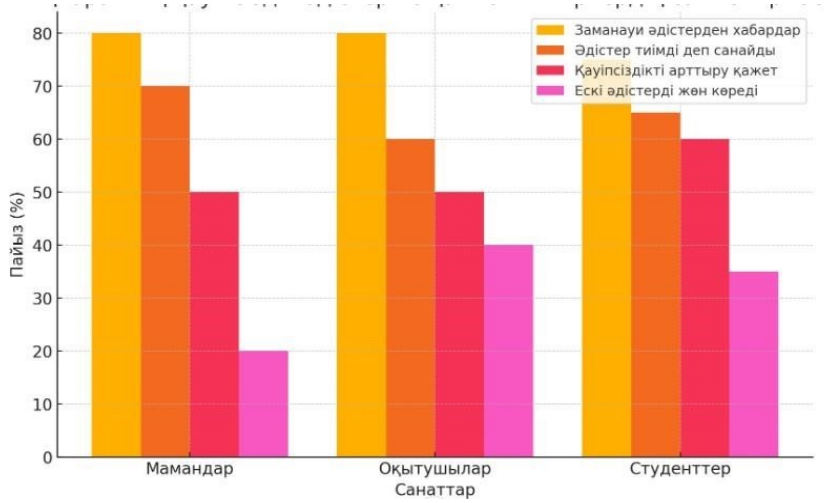
3-сурет. Студенттердің ойы диаграмма түрінде

Зерттеу нәтижелері көрсеткендей, ақпараттық жүйелерді қорғаудың заманауи әдістерін қолдану қажеттілігі барлық мүдделі тараптар арасында кеңінен қолдау тапқанымен, белгілі бір мәселелер де бар.Себебі зерттеу нәтижелері ақпараттық жүйелерді қорғаудың заманауи әдістерін белсенді түрде енгізу және оларды оқыту үдерісін жетілдіру қажеттігін дәлелдейді. Мамандар, оқытушылар және студенттер арасындағы ынтымақтастықты нығайту, сондай-ақ тәжірибелік оқыту мүмкіндіктерін кеңейту – болашақта осы салада тиімді кадрлар даярлаудың маңызды факторы болмақ.Сонымен қатар , төменде мамандар, оқытушылар және студенттердің ақпараттық жүйелерді қорғау әдістеріне қатысты көзқарастарын көрсеттім. Талдау барысында келесі негізгі аспектілер 4-суретте қарастырылған.

Бұл бағандық диаграмма зерттеуге қатысқан мамандардың, оқытушылардың және студенттердің ақпараттық қауіпсіздік әдістеріне қатысты пікірлерін салыстырады. Диаграммадағы әрбір түсті баған белгілі бір жауап нұсқасын білдіреді:

1. Заманауи әдістерден хабардар – мамандар мен оқытушылардың 80%-ы, ал студенттердің 75%-ы заманауи әдістерді білетінін айтты.

2. Әдістер тиімді деп санайды – мамандардың 70%-ы, оқытушылардың 60%-ы және студенттердің 65%-ы заманауи әдістердің тиімді екенін атап өтті.
3. Қауіпсіздікті арттыру қажет – мамандар мен оқытушылардың 50%-ы және студенттердің 60%-ы ақпараттық жүйелерді қорғауда заманауи әдістерді қолдану қауіпсіздікті арттырады деп есептейді.
4. Ескі әдістерді жөн көреді – мамандардың 20%-ы, оқытушылардың 40%-ы және студенттердің 35%-ы бұрынғы әдістерді тиімді деп санап, жаңа әдістерге толық сенбейтіндерін білдірді.



4-сурет. Мамандар, оқытушылар және студенттердің АЖ қорғау әдістеріне көзақарстары баған түрінде

Талқылау

Жоғарыда зерттеу нәтижесі көрсеткендей көрсеткендей, мамандар, оқытушылар және студенттер заманауи ақпараттық қауіпсіздік әдістерін дамыту қажеттігін қолдайды. Әсіресе, мамандар мен оқытушылардың көпшілігі жаңа әдістермен таныс және оларды тиімді деп есептейді. Сонымен қатар, студенттер қауіпсіздік шараларын жетілдіру керектігін ерекше атап өткен. Алайда, барлық топтарда белгілі бір бөлігі ескі әдістерді артық көреді, бұл жаңа технологияларды енгізу барысында қосымша түсіндіру жұмыстарын жүргізу қажет екенін көрсетеді.

Қорытынды

Ақпараттық жүйелерді қорғаудың заманауи әдістерін зерттеу нәтижелері олардың киберқауіпсіздікті қамтамасыз етуде маңызды рөл атқаратынын көрсетті. Криптографиялық әдістер, көпфакторлы аутентификация, зиянды бағдарламалардан қорғау, желілік қауіпсіздік құралдары және қауіп-қатерлерді анықтау мен алдын алу жүйелері ақпараттық жүйелердің тұрақтылығы мен қорғанысын арттыруға көмектеседі.

Зерттеу нәтижелері көрсеткендей, мамандар, оқытушылар және студенттер ақпараттық жүйелерді қорғаудың жаңа әдістерін енгізу қажеттілігін қолдайды. Алайда, кейбір мамандар мен студенттер дәстүрлі әдістердің тиімділігіне сенім артады, бұл жаңа технологияларды енгізу барысында қосымша түсіндіру жұмыстарын жүргізу керектігін көрсетеді.

Сонымен қатар, зерттеу нәтижелері ақпараттық қауіпсіздік бойынша оқыту үдерісін жетілдіру қажеттілігін айқындады. Студенттердің көпшілігі тек теориялық біліммен шектелмей, практикалық дағдыларды дамытуға мүдделі екенін білдірді. Осыған байланысты, ақпараттық жүйелерді қорғау саласында тәжірибеге негізделген оқыту әдістерін қолдану маңызды болып табылады.

Жалпы, ақпараттық жүйелерді қорғаудың заманауи әдістерін қолдану ұйымдардың ақпараттық қауіпсіздігін нығайтуға, кибершабуылдар мен деректердің жоғалу қаупін азайтуға мүмкіндік береді. Болашақта бұл әдістерді жетілдіру және оларды білім беру жүйесіне кеңінен енгізу ақпараттық қауіпсіздік саласындағы мамандардың кәсіби деңгейін арттыруға ықпал етеді.

Пайдаланылған әдебиеттер тізімі

1. Белявский, А. (2021). *Криптографиялық әдістер мен олардың ақпараттық қауіпсіздіктегі рөлі*. Журнал «Ақпараттық қауіпсіздік».
2. Касперский, Ю. (2020). *Зиянды бағдарламалардан қорғау және олармен күрес әдістері*. Kaspersky Lab.
3. Ли, В., & Чен, Л. (2018). *Желілік қауіпсіздік және оның қорғау әдістері*. ScienceDirect.
4. Xie, Z., & Wu, B. (2019). *Security and Privacy in Multifactor Authentication Systems*. ResearchGate.
5. Кавва, П., & Лехал, Г. С. (2021). *Ақпараттық жүйелердегі қауіп-қатерлерді анықтау және алдын алу*. Springer.
6. Liu, H., & Zhang, S. (2020). *Artificial Intelligence for Information System Security*. ScienceDirect.
7. Stallings, W. (2018). *Cryptography and Network Security: Principles and Practice*. Pearson Education.
   (*Криптография және желілік қауіпсіздік: қағидалар мен тәжірибе*).
8. Kaufman, C., Perlman, R., & Speciner, M. (2016). *Network Security: Private Communication in a Public World*. Prentice Hall.
9. ISO/IEC 27001:2022. *Information Security Management Systems – Requirements*. International Organization for Standardization.
10. Танэнбаум А.С. (2017). *Таратылған жүйелер: қағидалар мен парадигмалар*

СОВРЕМЕННЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ

А.С. Наби

Научный руководитель: Н.А. Курмангалиева

В настоящее время безопасность и защита информационных систем стали важнейшим вопросом для любой организации. Современные методы защиты информационных систем требуют применения различных инструментов и технологий для обеспечения безопасности данных и повышения устойчивости систем к внешним атакам. В данной статье рассматриваются основные современные методы, применяемые для обеспечения безопасности информационных систем. К ним относятся криптографические методы, многофакторная аутентификация, системы защиты от вредоносного ПО, средства сетевой безопасности, а также системы обнаружения и предотвращения угроз. Кроме того, рассматриваются новые подходы к защите данных и инновационные технологии, применяемые для повышения безопасности информационных систем. Эффективное использование методов защиты информационных систем позволяет обеспечить информационную безопасность организаций и снизить риски, связанные с кибератаками и потерей данных. Особенно важную роль в повышении эффективности информационной безопасности играют внедрение новых технологий и развитие в данной области. Методы и решения, рассмотренные в статье, отражают актуальные вопросы обеспечения безопасности информационных систем и перспективные направления их развития.

Ключевые слова: информационные системы, криптография, многофакторная аутентификация, сетевая безопасность, кибератаки, инновационные технологии.

MODERN METHODS OF INFORMATION SYSTEMS SECURITY

A.S. Nabi

Scientific Advisor: N.A. Kurmangaliyeva

Nowadays, the security and protection of information systems have become a critical issue for any organization. Modern methods of information system protection require the use of various tools and technologies to ensure data security and enhance

system resilience against external attacks. This article explores the main contemporary methods used to secure information systems. These include cryptographic methods, multi-factor authentication, malware protection systems, network security tools, as well as threat detection and prevention systems. In addition, the paper examines new approaches to data protection and innovative technologies used to enhance the security of information systems. The effective application of these methods enables organizations to ensure their information security and reduce risks associated with cyberattacks and data loss. The introduction of new technologies and advancements in this field play a particularly important role in improving the effectiveness of information security. The methods and solutions discussed in this article highlight current issues in information system security and outline promising directions for future development.

Keywords: information systems, cryptography, multi-factor authentication, network security, cyberattacks, innovative technologies.

REFERENCES

1. Belyavsky, A. (2021). Cryptographic methods and their role in information security. *Journal "Information Security"*.
2. Kaspersky, Y. (2020). Protection against malicious software and methods of combating it. *Kaspersky Lab*.
3. Li, V., & Chen, L. (2018). Network security and its protection methods. *ScienceDirect*.
4. Xie, Z., & Wu, B. (2019). Security and Privacy in Multifactor Authentication Systems. *ResearchGate*.
5. Kavva, P., & Lehal, G. S. (2021). Detection and prevention of threats in information systems. *Springer*.
6. Liu, H., & Zhang, S. (2020). Artificial Intelligence for Information System Security. *ScienceDirect*.
7. Stallings, W. (2018). *Cryptography and Network Security: Principles and Practice*. Pearson Education.
8. Kaufman, C., Perlman, R., & Speciner, M. (2016). *Network Security: Private Communication in a Public World*. Prentice Hall.
9. ISO/IEC 27001:2022. *Information Security Management Systems – Requirements*. International Organization for Standardization.
10. Tanenbaum, A. S. (2017). *Distributed Systems: Principles and Paradigms*.