EKTU JOURNAL OF INFORMATION AND COMMUNICATION SCIENCES

https://doi.org/10.51885/3134-8025_JICS_2026_2_6
ХҒТАР 81.93.29

# МЕТАУНИВЕРСИТЕТТЕГІ ҚҰПИЯЛЫЛЫҚ ЖӘНЕ ДЕРЕКТЕРДІ ҚОРҒАУ: VR СЫНЫПТАРЫ МЕН ӘЛЕМДІК ЧАТТЫ ҚОРҒАУ

# КОНФИДЕНЦИАЛЬНОСТЬ И ЗАЩИТА ДАННЫХ В МЕТАУНИВЕРСИТЕТЕ: ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ VR-КЛАССОВ И ВНУТРЕННЕГО ЧАТА

# PRIVACY AND DATA PROTECTION IN METAUNIVERSITY: SECURING VR CLASSROOMS AND IN-WORLD CHAT

**М.Т. Ипалакова[1], Д.О. Шарипов[1], Д.Д. Цой[1], Е.А.Дайнеко[2], A.D. Samala[3]**
[1]Халықаралық ақпараттық технологиялар университет, Алматы, Қазақстан
[2]Автоматика және ақпараттық технологиялар институты, Сәтбаев университеті, Алматы, Қазақстан
[3]Негери Паданг университеті, Батыс Суматра, Паданг, Индонезия
Жауапты автор: Цой Дана Дмитриевна, e-mail: d.tsoy@iitu.edu.kz

**Түйінді сөздер:**
Метауниверситет, виртуалды шындық аудиториясы, чат, құпиялылық, деректерді қорғау, RBAC, шифрлау, модерация, криминалистика.

**ТҮЙІНДЕМЕ**
Бұл мақалада VR сыныптарын, ішкі мәтіндік/дауыс чатын және оқу нәтижелерін университеттің ақпараттық жүйелерімен синхрондауды біріктіретін білім беру метауниверситетіндегі деректердің құпиялылығы мен қорғалуы қарастырылады. Онда мұндай платформалардың қауіпсіздігі келесі қауіптердің үйлесімімен анықталатыны көрсетілген: тіркелгі мен аватардың бұзылуы, XR телеметриясы мен биосигналдың ағып кетуі, интеграция және желілік синхрондау тәуекелдері және әлеуметтік-техникалық коммуникацияларды теріс пайдалану. Зерттеудің мақсаты - ақпараттың құпиялылығы мен тұтастығын нақты уақыт режимінде қамтамасыз ететін қайталанатын деректер мен коммуникация қауіпсіздігі архитектурасын әзірлеу. Әдістеме деректерді жіктеуді, қауіпті модельдеуді және құпиялылық бойынша дизайн парадигмасы шеңберінде кіру саясатын ресімдеуді қамтиды. Ұсынылған архитектураға SSO/MFA/RBAC, чат және VR сессиясын модерациялау, сыртқы ақпараттық жүйелермен қауіпсіз интеграция, криптографиялық қорғау (TLS, AES-GCM, KMS/HSM) және журнал жүргізу/криминалистикалық тізбек (SIEM, өзгермейтін аудит журналдары) кіреді.

**Ключевые слова:**
метауниверситет, виртуальная аудитория, чат, конфиденциальность, защита данных, RBAC, шифрование, модерация, форензика.

**АННОТАЦИЯ**
Статья рассматривает обеспечение конфиденциальности и защиты данных в образовательном метауниверситете, объединяющем VR-классы, внутренний текстовый/голосовой чат и синхронизацию учебных результатов с университетскими информационными системами. Показано, что безопасность таких платформ опре-деляется связкой угроз: компрометацией аккаунтов и аватаров, утечками XR-телеметрии и биосигналов, рисками интеграций и сетевой синхронизации, а также социально-техническими злоупот-

реблениями в коммуникациях. Цель работы – разработать воспроизводимую архитектуру защиты данных и коммуникаций, обеспечивающую конфиденциальность и целостность информации в режиме реального времени. Методология включает классификацию данных, моделирование угроз и формализацию политик доступа в парадигме privacy-by-design. Предложена архитектура, включающая SSO/MFA/RBAC, модерацию чата и VR-сессий, защищённую интеграцию с внешними ИС, криптографическую защиту (TLS, AES-GCM, KMS/HSM) и контур логирования/форензики (SIEM, неизменяемые аудит-логи).

**keywords:**
Metauniversity, virtual reality classroom, chat, privacy, data protection, RBAC, encryption, moderation, forensics.

**ABSTRACT**
This article examines privacy and data protection in metauniversity that integrates VR classrooms, internal text/voice chat, and the synchronization of learning outcomes with university information systems. It demonstrates that the security of such platforms is determined by a combination of threats: account and avatar compromise, XR telemetry and biosignal leaks, integration and network synchronization risks, and sociotechnical communications abuse. The goal of the study is to develop a reproducible data and communications security architecture that ensures the confidentiality and integrity of information in real time. The methodology includes data classification, threat modeling, and the formalization of access policies within the privacy-by-design paradigm. The proposed architecture includes SSO/MFA/RBAC, chat and VR session moderation, secure integration with external information systems, cryptographic protection (TLS, AES-GCM, KMS/HSM), and a logging/forensics circuit (SIEM, immutable audit logs).

## КІРІСПЕ

VR сыныптары мен интеграцияланған байланыс арналары (мәтін, дауыс, медиа) бар заманауи білім беру метакеңістіктері XR сенсорларын, идентификациясын, оқу аналитикасын және байланыс қызметтерін біріктіреді. Сондықтан олардың қауіпсіздігі бір ішкі жүйемен емес, қауіптердің үйлесімімен анықталады. Жалпы метакеңістік архитектурасы деңгейінде негізгі тәуекелдерге тіркелгі мен аватардың бұзылуы, мазмұн мен көрініс ауыстыру, желілік синхрондау шабуылдары, үшінші тарап қызметінің осалдықтары және телеметрия деректерінің ағып кетуі жатады. Виртуалды ортада қудалау, қорқыту және манипуляцияны қоса алғанда, әлеуметтік қорлау да маңызды (Abedin et al., 2022). VR және AR-дың ерекше сипаты ағып кетулердің салдарын күшейтеді. Тек жеке деректер ғана емес, сонымен қатар мінез-құлық және биометриялық сигналдар да қауіп астында, және оларды оқиғадан кейін анонимдеу қиын (Al-kaeed, Qayyum & Qadir, 2024).

Метакеңістік тәуекелдерін жүйелі шолу VR құрылғыларының, жасанды интеллект модульдерінің және интеграциялардың қиылысуын көрсетеді. Білім беру үшін бұл оқушылардың әрекет деректеріне, мысалы, көзқарасқа, қимылдарға, қозғалыстарға және мінез-құлық үлгілеріне жоғары сезімталдықты білдіреді. Бағалау және мұғалім мен оқушының өзара әрекеттесуінің контексті де маңызды (Al-kfairy et al., 2025). Метаверстің шолу зерттеулері қауіптердің көбінесе жүйелік деңгейлер арасында «ағып» кететінін көрсетеді. Сондықтан, көп деңгейлі қауіпсіздік моделі пайдалы. Ол құрылғыларды, желіні, сәйкестендіруді, деректерді және қолданбаларды қамтиды (Laiz-Ibanez, Mendaña-Cuervo & Carus Candas, 2025). Мұны толықтыра отырып, метаверс үшін қауіпсіздік және құпиялылық талаптарын зерттеу оларға қол жеткізуді бақылау, деректерді қорғау, аудит және теріс пайдалануға қарсы тұру сияқты тексерілетін шарттар ретінде қарастыруды ұсынады. Бұл тәсіл талаптарды білім беру VR қызметтерін жобалауға аударуды жеңілдетеді (Ren et al., 2024).

VR сыныбы үшін «деректерді қорғау» ғана емес, сонымен қатар ақпарат ағындары үшін контекстік нормаларды сақтау да маңызды. Деректерге кімнің және қандай жағдайларда қол жеткізе алатынын анықтау қажет. Контекстік тұтастық тәсілі VR сабақтарының жаңа деректер арналарын — кеңістіктік оқиғалар мен жеке өзара әрекеттесулерді жасайтынын көрсетеді. Бұлар білім берудегі құпиялылыққа деген үміттерге қайшы келуі мүмкін (Brehm & Shvartzhnaider, 2024). Бұл практикалық талаптарға әкеледі. Рөлдер мен өкілеттік шекаралары, жиналған сигналдарды азайту, сондай-ақ қол жеткізуді тіркеу және анық хабарландырулар қажет (Brehm & Shvartzhnaider, 2024).

XR биометриясымен тәуекелдердің бөлек класы байланысты. Көз деректері әсіресе маңызды. Ол интерфейстерде және бейімделгіш оқытуда қолданылады. Зерттеулер деанонимизация қаупін көрсетеді. Сондықтан, ресми құпиялылық шаралары қажет. Дифференциалды құпиялылық пен деректерді синтездеуге негізделген тәсілдер перспективті (Dutta, Lanvin & Wunsch-Vincent, 2022). Сонымен қатар, интерактивті VR үшін жеке ағынды деректерді пайдалану әдістері ұсынылады. Олар тұрақтылық пен пайдаланушы тәжірибесіне әсер етуді ескере отырып бағаланады (Shen et al., 2019). Мета-университет үшін бұл қарапайым ережеге әкеледі. Оқу көрсеткіштері шикі биосигналдардан бөлінуі керек. Тек қажетті минимум сақталуы керек. Мүмкіндігінше агрегация және жеке түрлендірулер қолданылуы керек (Dutta, Lanvin & Wunsch-Vincent, 2022).

Кіріктірілген чат және медиа бөлісу құпиялылық пен қауіпсіздік арасында шиеленіс тудырады. Толық шифрлау ұстап алу қаупін азайтады. Дегенмен, бұл зиянды мазмұнды анықтауды қиындатады. Сондықтан «жеке тексеру» схемалары ұсынылады. Бұлар мазмұнды толық ашпай-ақ зиянды анықтауға мүмкіндік береді. Криптографиялық хаттамалар және жеке медиа өңдеу қолданылады. Бұл білім беру үшін маңызды сала. «Бақылау үшін құпиялылықты өшіруге» болмайды. Дизайндық компромисс пен ашық процедуралар қажет (Garg et al., 2023).

Байланыс қауіпсіздігі әлеуметтік-техникалық қабатты қамтиды. Оларға уыттылық, модерация қателері және кемсітушілік әсерлер жатады. Уытты сөйлеуді анықтаудағы бейтараптыққа шолулар пайдаланушы топтары мен контексттер бойынша жүйелі қателіктерді көрсетеді (Giaretta, 2024). Сондықтан, білім беру чаттары үшін жергілікті валидация, ашық критерийлер және адамның бақылауы маңызды. Әділдік көрсеткіштері де қажет (Giaretta, 2024). Уытты жіктеудегі бейтараптыққа қосымша шолулар бейтараптықтың себептерін және оны азайту жолдарын жүйелейді. Олар модельдер мен процедураларды үнемі қайта бағалау қажеттілігін атап көрсетеді (Wang et al., 2023). Метаверс кластарын қабылдаудың эмпирикалық зерттеулері сенім, құпиялылық және әділдік арасындағы байланысты көрсетеді. Бұл платформаны пайдалануға дайындыққа әсер етеді (Laiz-Ibanez, Mendaña-Cuervo & Carus Candas, 2025). Соңында, тәуекелдер, гарнитуралар мен сессиялар деңгейінде күшейеді. Қорғалған тіркелгі болса да, құрылғының бұзылуы мүмкін. Сондықтан, AR және VR-дағы аутентификация бойынша зерттеулер үздіксіз және байқалмайтын пайдаланушыны тексеру механизмдерін ұсынады. Бір мысал - гарнитура қауіпсіздігі үшін жүріске негізделген аутентификация (Wilson et al., 2024). Бұл дәстүрлі шараларды толықтырады және сессияны ұрлау қаупін азайтады.

VR қауіпсіздігі мен құпиялылығына жалпы шолулар қауіптер мен әсерлерді жүйелейді. Олар типтік шабуылдарды, осалдықтардың себептерін және ашық мәселелерді атап көрсетеді. Бұл зерттеулер білім беру платформасын жобалау алдында базалық тәуекел картасы ретінде пайдалы (Zheng, Zhou, Lu & Cai, 2023). Оқу мәтіндік және дауыстық байланысты қолдайтын виртуалды сыныптарда өтетін білім беру метакеңістіктерін дамыту аясында, Құпиялылық және деректерді қорғау мәселелері жүйелік сипатқа ие болуда. Дәстүрлі LMS платформаларынан айырмашылығы, VR сыныптары оқушылар үшін кеңейтілген сандық із қалдырады: оқу нәтижелері мен хабарламалармен қатар, өзара

әрекеттесу деректері, мінез-құлық телеметриясы және қатысу оқиғалары жазылады. Бұл рұқсатсыз кіру, ақпараттың ағып кетуі, оқу нәтижелерінің бұрмалануы және байланыс арналарын теріс пайдалану қаупін арттырады. Сондықтан, мета-университеттегі қауіпсіздікті әртүрлі шаралар жиынтығы ретінде емес, кіруді басқаруды, коммуникация қауіпсіздігін, деректерді сақтау саясатын және оқиғаларға жауап беру процедураларын байланыстыратын тұтас архитектура ретінде қарастыру керек.

Бұл мақалада зерттеу нысаны метакеңістік, атап айтқанда, VR сыныптары мен ішкі чатты коммуникация құралы ретінде қамтитын сандық платформа ретіндегі мета-университет болып табылады.

Зерттеудің тақырыбы - VR сыныптарында және интеграцияланған чаттарда, соның ішінде университеттің ақпараттық жүйелерімен интеграциялау сценарийлерінде оқушылардың деректері мен байланыстарына құпиялылықты, тұтастықты және бақыланатын қол жеткізуді қамтамасыз ету әдістері мен архитектуралық шешімдері. Сондықтан, зерттеудің негізгі мақсаты - нақты уақыт режимінде деректердің құпиялылығы мен тұтастығын қамтамасыз ете алатын мета-университет үшін деректер мен коммуникация қауіпсіздігі архитектурасын әзірлеу және тексеру.

Осы мақсатқа жету үшін келесі зерттеу мақсаттары анықталды:

1. Мета-университет деректерін сезімталдық деңгейі бойынша жіктеу, сақтау және өңдеу талаптарын анықтау;

2. Білім беру сценарийлерін ескере отырып, қауіп моделін құру;

3. Аутентификация және кіруді бақылау механизмдерін (RBAC), арналардағы және тыныштықтағы деректерді шифрлауды, кілттерді басқаруды және маңызды әрекеттерді аудиттеуді қамтитын қауіпсіздік архитектурасын әзірлеу.

4. Құпиялылық қағидаттарын сақтай отырып, модерация және оқиғаларды тергеу механизмдері бар қауіпсіз ішкі чат жүйесін ұсыну;

5. Ұсынылған тәсілдің қолданылуын техникалық және ұйымдастырушылық критерийлерге сүйене отырып бағалау.

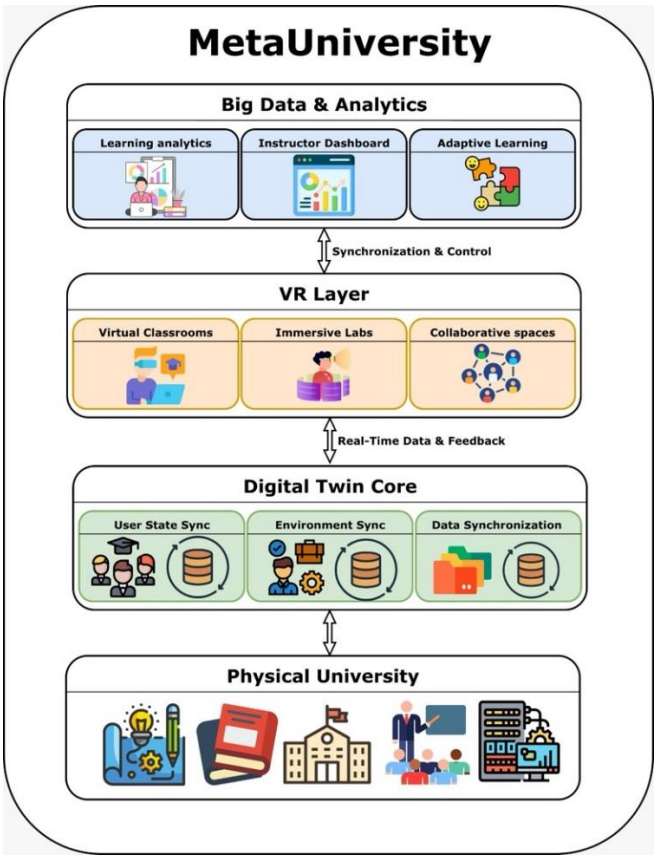
Бұл жобада қолданылатын әдістерге деректерді жіктеу және кіру саясатын ресімдеу, сондай-ақ қауіпсіздік механизмдерінің архитектуралық дизайны кіреді. Бұл тәсіл бізге қауіпсіздік шаралары жиынтығын сипаттауға ғана емес, сонымен қатар зерттеудің ғылыми жаңалығын анықтайтын қауіпсіз білім беру VR платформасын құрудың қайталанатын әдіснамасын ұсынуға мүмкіндік береді.

## ЗЕРТТЕУ МАТЕРИАЛДАРЫ МЕН ӘДІСТЕРІ

Виртуалды шындық (VR) және кеңейтілген шындық (XR) технологиялары иммерсивті, интерактивті оқу тәжірибесін жеңілдету арқылы педагогикалық нәтижелерді жақсартудың айтарлықтай әлеуетін көрсетті. Білім беру мекемелері көбінесе географиялық жағынан шашыраңқы халыққа қызмет көрсететін және физикалық ресурстарға шектеулерге тап болатын Қазақстан жағдайында VR модельденген зертханаларды, тарихи реконструкцияларды және бірлескен топтық жұмысты қоса алғанда, озық оқыту әдістеріне тең қол жеткізу мүмкіндіктерін ұсынады.

Metauniversity платформасы білім берудегі қолданыстағы VR жүйелеріндегі анықталған олқылықтарды, әсіресе статикалық, алдын ала рұқсат етілген 3D активтерге және нақты уақыт режиміндегі көп пайдаланушылы өзара әрекеттесудегі шектеулерге тәуелділікті жоюға арналған. Жоба сұраныс бойынша 3D нысандарын генерациялауға арналған заманауи жасанды интеллект модельдерін интуитивті қимыл және дауыс негізіндегі интерфейстермен біріктіру арқылы тұтынушы деңгейіндегі автономды құрылғыларда динамикалық мазмұн жасауды және үздіксіз ынтымақтастықты қамтамасыз етуге бағытталған.

Бұл бастама информатика, инженерия, мәдениеттану және медициналық оқытуды қоса алғанда, әртүрлі пәндер бойынша қолданылатын масштабталатын құралды әзірлеу бойынша тәуелсіз зертханалық күш-жігерді біледіреді. Ол зертхананың VR өзара әрекеттесу жүйелеріндегі бұрынғы тәжірибесіне сүйене отырып, генеративтік жасанды интеллект пен желілік виртуалды ортадағы заманауи жетістіктерді біріктіреді.




**1-сурет.** Метауниверситет тұжырымдамасының модульдері
*Ескерту – авторлар құрастырған*

Зерттеу 1-суретте көрсетілген MetaUniversity тұжырымдамасын әзірлеуге негізделген, ол сандық егіз және аналитикалық тізбек арқылы физикалық университетке қосылған білім беру метакеңістігінің көп қабатты архитектурасы ретінде. Тұжырымдама төрт өзара байланысты қабаттар жүйесі ретінде қалыптасты: (1) Физикалық университет (нақты білім беру процестері мен инфрақұрылымы), (2) Сандық егіз ядро (пайдаланушы күйлерін, орталарын және деректерді синхрондау), (3) VR қабаты (виртуалды сыныптар, иммерсивті зертханалар және бірлескен кеңістіктер) және (4) Үлкен деректер және аналитика (оқу аналитикасы, нұсқаушының басқару тақталары және бейімделгіш оқыту). Тұжырымдаманың екі түрі байланыстардың кілті болып табылады: аналитикалық қабат пен VR қабаты арасындағы синхрондау және басқару (оқытуды басқару және бейімдеу) және VR қабаты мен сандық егіз ядросы арасындағы нақты уақыттағы деректер және кері байланыс (әрекеттерді, оқиғаларды және нәтижелерді нақты уақыт режимінде жазу). Бұл орнату бізге жүйелік құпиялылық талаптарын орнатуға мүмкіндік берді: платформа тек «VR көрінісін көрсетіп қана қоймай», сонымен қатар қабаттар арасында деректерді үздіксіз алмастырады, сондықтан қауіпсіздік тек бір қызметте ғана емес, бүкіл архитектура бойынша деректер ағындары мен рөлдер деңгейінде қамтамасыз етілуі керек.

**НӘТИЖЕЛЕР ЖӘНЕ ОЛАРДЫ ТАЛҚЫЛАУ**

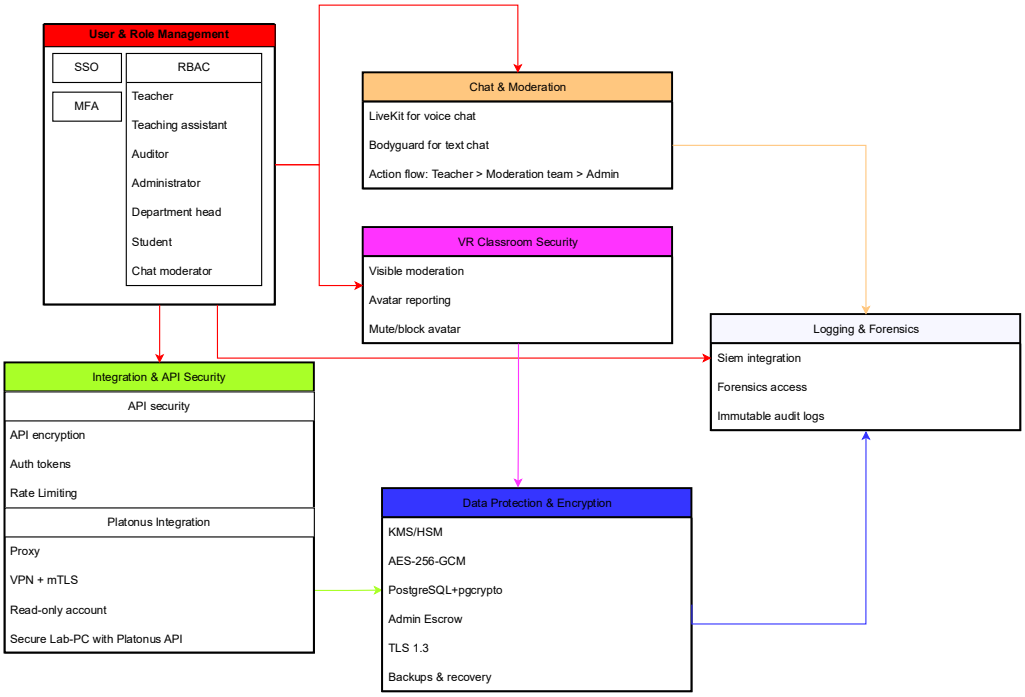
Metaverse басқару тәсілдері екі архитектуралық санатқа бөлінеді: орталықтандырылған және орталықтандырылмаған. Орталықтандырылған платформалар (Web2) бір ғана нысанмен басқарылады, бұл жоғары өнімділікті, қатаң мазмұнды модерациялауды және оңай интеграцияны қамтамасыз етеді. Екінші жағынан, орталықтандырылмаған Web3 архитектуралары икемдірек және виртуалды активтерге иелік етуге мүмкіндік береді, бірақ кіруге үлкен кедергі келтіреді, тұрақсыз және әрқашан қауіпсіз бола бермейді (Chen, 2023). Платформаны таңдау мақсатты аудитория мен мақсаттарға байланысты. Орта және STEM білім беру үшін Minecraft Education және Roblox сияқты орталықтандырылған платформалар жүйелік талаптары төмен геймификацияланған ортаны ұсынған қолайлырақ (Minecraft, 2026; Roblox, 2026). Жоғары білім беру және корпоративтік оқыту үшін Engage VR маңыздырақ. 1-кестеде әртүрлі метаплатформалар олардың архитектурасына, бағытына, артықшылықтары мен кемшіліктеріне негізделе салыстырылады (Engage, 2026).

**1-кесте.** Метаплатформаларды салыстыру кестесі

| Платформа | Сәулет өнері | Негізгі назар білім беруге аударылады | Артықшылықтары | Кемшіліктер |
|---|---|---|---|---|
| Minecraft білім беру / Roblox | Орталықтандырылған | Мектептегі білім беру, STEM, бағдарламалау, логика | Балаларға таныс орта, ойынға бейімделу, жүйелік талаптардың төмендігі | Жеңілдетілген «блок тәрізді» графика, ойын-сауық мазмұнының алаңдату қаупі |
| VR-ды қосыңыз | Орталықтандырылған | Жоғары білім, корпоративтік оқыту, күрделі модельдеу | Дәріскерлерге арналған кәсіби құралдар, реалистік физика, білім беру стандарттарымен интеграция | Толық тәжірибе алу үшін қымбат VR гарнитуралары қажет |
| Кеңістіктік | Орталықтандырылған | Жобалық жұмыс, виртуалды көрмелер, ынтымақтастық | Браузер арқылы (VR жоқ), кросс-платформалар, фотореалистік аватарлар арқылы оңай қол жеткізу | Ресми тестілеу мен емтихандарды өткізуге арналған шектеулі функционалдылық |
| Орталықсыздандырылған жер / Құмсалғыш | Орталықсыздандырылған (Web3) | Web3 технологияларын, экономикасын, цифрлық өнерді зерттеу | Жасалған кеңістікті толық бақылау, студенттік жобаларды монетизациялау | Кіру шегі жоғары (крипто әмияндар қажет), қажетсіз мазмұнды модерациялау қиын |

*Ескерту – авторлар құрастырған*

Meta-University қауіпсіз жұмысын қамтамасыз ету үшін 2-суретте көрсетілгендей, орталықтандырылған архитектураны жүзеге асыратын пайдаланушы деректерін қорғау тәсілі әзірленді.




**2-сурет.** Метауниверситет тұжырымдамасының модульдері
*Ескерту – авторлар құрастырған*

Диаграммада метауниверситеттегі құпиялылық пен деректерді қорғауды қамтамасыз етудің ұсынылған архитектурасы көрсетілген, мұнда оқыту VR аудиториясында өткізіледі және ішкі коммуникациялармен (мәтін/дауыс) қолдау көрсетіледі, ал білім беру деректері сыртқы университет жүйесімен (Platonus) синхрондалады. Тұжырымдама өзара байланысты циклдар жиынтығы ретінде құрылымдалған, олардың әрқайсысы белгілі бір тәуекелдер жиынтығына жауап береді: сәйкестік пен құқықтарды басқару, VR-дағы коммуникациялар мен мінез-құлық қауіпсіздігі, интеграция және API қорғау, криптографиялық деректерді қорғау және, соңына келгенде, оқиғаларды тергеуге арналған тіркеу және криминалистика.

Жоғарғы сол жақ блокта сенім мен бақылаудың негізін қалайтын Пайдаланушы және рөлдерді басқару циклі көрсетілген. Аутентификация SSO арқылы жүзеге асырылады және MFA арқылы күшейтіледі, ал платформа функцияларына қол жеткізу RBAC көмегімен ұйымдастырылады. Рөлдік модель негізгі білім беру рөлдерін (Студент, Мұғалім) және операциялық және бақылау рөлдерін (Оқытушы көмекшісі, Чат модераторы, Аудитор, Әкімші, Кафедра меңгерушісі) қамтиды. Бұл жүйедегі деректер мен әрекеттерге кез келген қол жеткізуге (чат модерациясынан бастап сынып жазбаларын өңдеуге дейін) тек нақты анықталған құқықтар шеңберінде және ең аз артықшылық қағидаты шеңберінде рұқсат етілетінін, ал маңызды операцияларды жақсартылған аутентификация мен аудитпен байланыстыруға болатынын білдіреді. Орталық, жоғарғы блок, Чат және Модерация, ішкі коммуникациялық құрылымды және оны басқаруды сипаттайды. Дауыстық арна дауыстық чат үшін LiveKit көмегімен жүзеге асырылады, ал мәтіндік арна мәтіндік чат модерациясы үшін Bodyguard компонентін пайдаланады. Диаграммада анықталған

оқиғаға жауап беру процесі маңызды ерекшелік болып табылады: Мұғалім → Модерация тобы → Админи. Бұл бастапқы жауап беру және зиянның алдын алу мұғалім немесе сынып жетекшісі деңгейінде жүзеге асырылатынын, содан кейін модерация тобы қатысатынын және әкімші тек кеңейтілген өкілеттіктерді және ресми тергеуді қажет ететін істерге ғана қатысатынын білдіреді. Бұл схема әкімшілік құқықтарды теріс пайдалану қаупін азайтады, сонымен бірге жедел жауап беруді қамтамасыз етеді.

Төменде VR сынып қауіпсіздігі блогы берілген, ол VR сессиясындағы тікелей қауіпсіздік шараларын көрсетеді. Жүйеге көрінетін модерация (модератордың/мұғалімнің көрінетін қатысуы), мінез-құлық туралы хабарлау үшін аватар туралы хабарлау механизмдері және аватарларды өшіру/блоктау сияқты жылдам әрекет ету құралдары кіреді. Осылайша, VR сыныбының қауіпсіздігі тек техникалық шаралармен ғана емес, сонымен қатар нақты уақыт режимінде мінез-құлықты бақылаудың әлеуметтік және техникалық механизмдерімен де қамтамасыз етіледі, бұл қорқыту немесе қорлау қаупі бар жоғары интерактивті білім беру ортасы үшін өте маңызды.

Төменгі сол жақтағы Интеграция және API қауіпсіздігі блогы сыртқы қызметтермен және жүйелермен өзара әрекеттесу үшін қауіпсіз периметрді құрайды. API деңгейінде API шифрлау, аутентификация токендері және жылдамдықты шектеу қолданылады, бұл ұстап алу, сұранысты бұрмалау және автоматтандырылған шабуылдар қаупін азайтады. Бұл шеңберде прокси және қауіпсіз VPN + mTLS арнасы арқылы жүзеге асырылатын Platonus-пен интеграция да ерекшеленеді. Сонымен қатар, тәуекелді азайту принципі белгіленеді: тек оқуға арналған тіркелгіні пайдалану Platonus деректерін интеграция шеңберінен өзгерту мүмкіндігін шектейді, ал Platonus API бар Secure Lab-PC сценарийі сыртқы жүйеге тек белгіленген қауіпсіз жұмыс станциясынан кірудің практикалық шектеулерін қарастырады. Бұл дизайн интеграцияны басқарылатын, аудиттелетін және деректер алмасу интерфейсінің бұзылуына төзімді етеді.

Төменгі, орталық блок, Деректерді қорғау және шифрлау, деректердің құпиялылығы мен тұтастығының негізін білдіреді. Кілттерді басқару KMS/HSM жүйесінде жүзеге асырылады, ал қалған кезде деректерді шифрлау AES-256-GCM көмегімен жүзеге асырылады; сақтау PostgreSQL + pgcrypto жүйесінде қамтамасыз етіледі. TLS 1.3 қауіпсіз қосылымдар үшін қолданылады, ал ақауларға төзімділік сақтық көшірмелер мен қалпына келтіру механизмдерімен қолдау көрсетіледі. Әкімшінің деректерді кездейсоқ оқуының орнына, ресми және бақыланатын кіру процесі қажет болған ерекше жағдайларда (мысалы, оқиғаларды тергеу) қорғалған деректерге басқарылатын кіруді қамтамасыз ету үшін жеке механизм, әкімшілік эскроу, қарастырылған. Оң жақтағы журнал жүргізу және криминалистика блогы жүйенің бақылаулылығын және дәлелдемелерді қамтамасыз етеді. Оған орталықтандырылған оқиғаларды бақылау үшін SIEM интеграциясы, тергеу жүргізу үшін уәкілетті қызметкерлердің криминалистикаға кіруі және журналдарды өзгертуден немесе жоюдан қорғау механизмі ретінде өзгермейтін аудит журналдары кіреді. Диаграммадағы қосылымдар оқиғалар мен әрекет нәтижелерінің бұл циклге VR қауіпсіздігі мен деректерді қорғау ішкі жүйесінен кіріп, үздіксіз аудит тізбегін құрайтынын көрсетеді: бұзушылық немесе күдікті әрекет фактісінен бастап оны жазуға, талдауға және кейінгі әкімшілік шешімге дейін.

Осылайша, диаграмма тұтас модельді көрсетеді: рөлдерді басқару (SSO/MFA/RBAC) рұқсат етілген пайдаланушы әрекеттерін анықтайды; чат және VR сыныптары модерация және есеп беру механизмдерімен қорғалған; интеграциялар (соның ішінде Platonus) API және байланыс арнасы деңгейінде оқшауланған және қорғалған; деректер шифрланған және басқарылады.

Деректер KMS/HSM арқылы жиналады; барлық маңызды әрекеттер мен оқиғалар өзгермейтін журналдарда жазылып, бақылау және криминалистика үшін SIEM-ге жіберіледі.

Қауіпсіздік пен өнімділікті теңестіру үшін біз селективті шифрлауды енгізуді жоспарлап отырмыз: маңызды деректер (ID, токендер, аудио) AES-256-GCM арқылы қорғалады, ал XR телеметриясы жеңіл хаттамалармен қорғалады. Бұл VR иммерсиясын сақтай отырып, кідіріс уақытын қолайлы шектерде сақтайды.

Edge-негізделген модерация тұжырымдамасы толық журналдардың орнына тек шифрланған оқиға «жалаушаларын» алмасу арқылы серверге берілетін деректер көлемін азайтады, бұл қоршаған ортаның қауіпсіздігіне нұқсан келтірмей құпиялылықты қамтамасыз етеді.

Журналдың өзгермейтіндігін қамтамасыз ету үшін хэш ағаштары қолданылады. Блоктарды тізбекке хэштеу өнімділік немесе бұзушылық деректерін ретроспективті түрде өңдеудің алдын алады, бұл жүйенің аудиттер үшін ашықтығы мен сенімділігіне кепілдік береді.

Төмендегі 2-кестеде мета-университет ішінде жиналған және өңделген деректер көрсетілген. Әрбір деректер класы үшін мысалдар, сезімталдық деңгейлері, сақтау мерзімдері және рөл бойынша қолжетімділік берілген. Сезімталдық деңгейі ақпараттың ағып кетуі немесе дұрыс пайдаланылмауы жағдайындағы ықтимал залалды көрсетеді. Қолжетімділік үлгі бойынша анықталады: студент, оқытушы, әкімші және аудитор немесе ақпараттық қауіпсіздік қызметі. Деректер ішкі, құпия және өте сезімтал болып жіктеледі. Өте сезімтал деректер үшін қатаң ережелер қолданылады. Мұндай деректерді жинау шектеулі, сақтау мерзімдері қысқартылған және қол жеткізу тек қажет болған жағдайда ғана беріледі. Ұсынылған сақтау мерзімдерін университет саясаты мен ақпараттық қауіпсіздік талаптарына сәйкес реттеуге болады. Бұл матрица қауіп моделін құру және қауіпсіздік шараларын таңдау үшін одан әрі қолданылады.

**2-кесте.** Метауниверситетте жиналған және өңделетін деректер түрлері

| Класс деректер | Жиналған деректер түрі | Сезімтал-дық | Жарамдылық мерзімі | Рөлдерге кіру мүмкіндігі |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| Идентифика-циялық деректер | SSO - идентификатор, рөл, топ, сессия токендері | Құпия (PDn) | Университет/IS ережелері: тіркелгі белсенді болған кезде + мұрағат | IAM әкімшісі , аудитор; топтық тізімдер бойынша мұғалім |
| Профиль және аватар | Лақап ат, құпиялылық параметрлері, аватар опциялары | Ішкі/ құпия | Тіркелгі белсенді болған кезде; сұраныс бойынша жою | Пайдаланушы; модератор/әкім ші - қажет болған жағдайда |
| VR сеансының деректері | идентификаторы , қатысушылар, уақыт белгілері, көрініс/модуль | Ішкі | 90–365 күн (сапа/оқиғаны шешу) | Мұғалім (жеке сыныптар), әкімші, аудитор |
| XR мінез-құлық телемет-риясы | Позициялар/траектор иялар, қимылдар, өзара әрекеттесулер | Өте сезімтал (мінез-құлықтық) | Әдепкі: 30–90 күн агрегаттары; "шикі" - сақтамаңыз немесе жөндеу үшін ≤7 күн | Аналитика - тек агрегаттар; қолжетімділік шектеулі |

2-кестенің соңы

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| Көзді бақылау / көзқарас | Фиксациялар, назар аудару үлгілері | Әсіресе сезімтал (биометриялық/ мінез-құлық) | Әдепкі бойынша сақтамаңыз; қажет болса, синтез/ DP немесе агрегаттар ≤30 күн | Тек рұқсат + аудитор арқылы |
| Хабарламалар (мәтіндік) | Хабарламалар, реакциялар, арна метадеректері | Құпия | 90–180 күн; тәртіптік істер үшін – ережелерге сәйкес | Қатысушылар; шағым модераторы; тергеу кезіндегі аудитор |
| Байланыс (дауыс) | Аудио ағыны, транскрипция (егер қосылған болса) | Өте сезімтал | Аудио әдепкі бойынша сақталмайды; транскрипция 30-90 күн бойы міндетті емес. | Қатысушылар; модератор/аудитор - ережелерге сәйкес |
| Оқу нәтижелері | Бағалар, тапсырмалар, қатысу | Құпия (PDn) | Университеттің/IS ережелеріне сәйкес | Студент (меншік), мұғалім (курс), ақпараттық технологиялар әкімшісі, аудитор |
| Оқиғалар және модерация | Есептер, шешімдер, дәлелдемелер базасы | Құпия | 1-3 жыл (немесе ережелерге сәйкес) | Модератор, қауіпсіздік әкімшісі, аудитор |
| Техникалық журналдар және аудит | Кіру, рөлді өзгерту, API оқиғалары | Ішкі/ құпия | 180 күн – 2 жыл | Қауіпсіздік/ аудитор |
| *Ескерту – авторлар құрастырған* | | | | |

Тәуекелдер VR сессияларының, сәйкестендірудің, оқу аналитикасының, коммуникациялардың және сыртқы интеграциялардың қиылысында туындайды. Сондықтан, бұл зерттеуде архитектуралық тәсіл таңдалды. Ол жүйені деректер ағындары мен рөлдерімен байланыстырылған қауіпсіздік ілмектерінің жиынтығы ретінде сипаттайды.

Басқа зерттеулермен салыстыру тұрақты негізгі тұжырымды көрсетеді. Бұл сигналдар бұзушылықтардың әсерін арттырады. Сондай-ақ, дербестендіру мен аналитика деректерді жинауды басқаратыны, құпиялылықты дизайн бойынша және қатаң кіруді бақылауды талап ететіні расталды. Бұл тәсілдің айырмашылығы - бұл ұғымдар бірыңғай операциялық құрылымға біріктірілген. Ол рөлдерді, деректер арналарын, шифрлауды, модерацияны және тергеулерді байланыстырады.

Нәтижесінде пайда болған әсер архитектуралық құрылыммен түсіндіріледі. Циклдерді бөлу бұзушылықтардың ықтималдығын азайтады. Әрбір қауіп класына нақты шаралар тағайындалады. VR сыныбына көрінетін модерация және жылдам әрекет ету механизмдері қосылды. Чат үшін жауап тізбегі анықталды. Интеграциялар үшін қауіпсіз периметр мен шлюз қарастырылған. Деректер үшін криптографиялық қорғау және

кілттерді басқару қолданылады. Оқиғалар үшін өзгермейтін журналдар мен криминалистика енгізілді. Бірге алғанда, бұл жеке шаралар жиынтығы емес, басқарылатын жүйені жасайды.

Құпиялылық пен модерация арасындағы тепе-теңдік ерекше маңызды. Бұл мақсаттар арасындағы қайшылық әдебиеттерде жиі талқыланады. Толық тексеру бақылауды арттырады, бірақ сенімді азайтады. Бұл зерттеуде ымыраға келу қабылданған. Сақталған деректерді шифрлау сақталады. Шифрланған деректерге қол жеткізу тек ережелерге сәйкес рұқсат етіледі. Модерация автоматты таңдау және адами тексеру арқылы гибридті процесс ретінде құрылады. Дауыс беру үшін транскриптке негізделген тәсіл ұсынылады. Бұл процедураларды стандарттауды және шешімдерді аудиттеуді жеңілдетеді.

Ол әдетте бөлек қарастырылатын бес міндетті біріктіреді:

1) Рөлдерді басқару;

2) Әлеуметтік-техникалық орта ретіндегі VR сессияларының қауіпсіздігі;

3) Бақыланатын модерациясы бар жеке чат;

4) Сыртқы ақпараттық жүйелермен қауіпсіз интеграциялар;

5) Оқу және тәртіп процесінің бөлігі ретінде журнал жүргізу және криминалистика.

Операциялық жауап беру ағыны да жаңа. Ол әкімшілік артықшылықтарды теріс пайдалану қаупін азайтады және сыныптағы жауап беру жылдамдығын арттырады.

Гипотеза архитектуралық негіздememен расталады. Деректерді жіктеу, қауіп модельдеу және RBAC, шифрлау, аудит және модерацияның үйлесімі құпиялылық пен тұтастықты жақсартады. Оқиғаларды басқару басқарылатын болып қала береді. Дегенмен, эмпирикалық тексеру әлі де шектеулі. Қазіргі түрінде бұл архитектуралық және әдіснамалық валидация. Ірі көлемді пайдаланушы эксперименттері мен жүктеме өлшемдері ұсынылған жоқ. Сондықтан сандық тиімділікті тек прототиптеуден кейін ғана бағалауға болады. Нәтижелердің дәлдігі мен сенімділігі стандартты криптографиялық примитивтер, кіруді бақылау және аудит және API үшін желілік өлшемдер сияқты қайталанатын механизмдерге негізделген. Бұл шешімдері тексерілуі мүмкін. Олардың дұрыстығы енгізуге және қолдауға байланысты. Негізгі шарттарға әкімшілік тәртіп, сапалы кілттерді басқару және кешенді журнал жүргізу жатады.

Қолданылу шектеулері жүйенің жұмыс істеу ерекшеліктеріне байланысты. Оқиғаларды тергеу процедуралары және өкілеттіктерді нақты бөлу қажет. Рөлдік модельді орнату және қызметкерлерді оқыту өте маңызды. Модерация модельдерін жергілікті түрде тексеру де қажет, себебі қателіктер мен әділетсіз тәжірибелер орын алуы мүмкін. Сыртқы ақпараттық жүйелермен интеграция интерфейстердің қолжетімділігіне және университет саясатына байланысты. Дауыстық деректерді жазуға және материалдарды сақтауға қатысты заңды талаптар өте маңызды.

Бір ықтимал шектеу - өнімділік пен қауіпсіздікті теңестіру қажеттілігі. Тым күрделі нақты уақыттағы шифрлау алгоритмдері пайдаланушы тәжірибесіне кері әсер етуі мүмкін.

Жүйені пайдаланушылар санының көп болуына масштабтау әкімшілік және модерация тұрғысынан жүйені басқаруға қысым жасайды. Бұл мәселені шешу үшін модераторлар құрамын кеңейту немесе автоматтандырылған бақылау жүйелерін енгізу қажет болуы мүмкін.

Тағы бір осалдық - сандық университет ішіндегі өзара әрекеттесу кезінде жиналған деректердің ерекше сипаты: биометриялық параметрлер, қозғалыс үлгілері және көзді бақылау жеке деректер туралы заңдарды сақтау тұрғысынан құқықтық қиындықтар тудырады. Сондықтан, метакеңістіктегі бұзушылықтар үшін құқықтық жауапкершілікті бөлу қажеттілігі бар.

Зерттеудің шектеулері бағалаудың толық еместігіне қатысты. Қазіргі уақытта кідіріс және қосымша көрсеткіштер, сондай-ақ қауіпсіздік шараларының VR сессиясының тұрақтылығына әсерін бағалау жетіспейді. Пайдаланушылардың хабарландырулар мен белгіленген ережелерге сенімі зерттелмеген. Бұл шектеулерді прототип әзірлеу, жүктемені тестілеу және пайдаланушыларды зерттеу арқылы шешу ұсынылады. Модерация процедуралары мен апелляциялық механизмдердің әділдігі бөлек қарастыруды қажет етеді.

Жұмысты одан әрі дамыту үш негізгі бағытта жоспарланған. Бірінші бағыт XR телеметриясының құпиялылықты сақтайтын аналитикасына қатысты және агрегация және деректерді азайту режимдерін пайдалануды қамтиды. Екінші бағыт әділ модерацияны қамтамасыз етуге арналған және тиісті көрсеткіштерді әзірлеуді, жергілікті деректер жиынтығын қалыптастыруды және адам-циклдегі тәсілдерді қолдануды қамтиды. Үшінші бағыт цифрлық әлемнің қауіпсіздігін қамтамасыз етуге бағытталған.

## ҚОРЫТЫНДЫ

VR/AR-дың ерекше сипаты құпиялылықтың бұзылуының салдарын күшейтеді, себебі тек жеке деректер ғана емес, сонымен қатар фактіден кейін сенімді түрде жасыру қиын мінез-құлық және биометриялық сигналдар (соның ішінде көзді бақылау) да қауіп астында. VR құрылғыларының, аналитикалық және бейімделгіш модульдердің және сыртқы интеграциялардың қиылысуын ескере отырып, құпиялылықты қамтамасыз ету құпиялылық бойынша дизайн тәсілдерін, бақыланатын қолжетімділікті, криптографиялық және статистикалық қорғау механизмдерін пайдалануды талап етеді.

Зерттеудің негізгі нәтижесі MetaUniversity тұжырымдамасын (1-сурет) сандық егіз және аналитикалық құрылым арқылы физикалық университетпен байланысты көп қабатты архитектура ретінде әзірлеу болды. Бұл тұжырымдама бізге жүйелік талапты ресімдеуге мүмкіндік берді: қауіпсіздік бүкіл архитектура бойынша деректер ағындары мен рөлдер деңгейінде қамтамасыз етілуі керек, себебі платформа қабаттар арасында үздіксіз деректер алмасады (VR сессиялары, күйді синхрондау, аналитика, кері байланыс) және оқушы үшін кеңейтілген сандық із қалдырады. Осы тұжырымдамаға сүйене отырып, пайдаланушы деректерін қорғаудың кешенді архитектурасы ұсынылады (2-сурет), оған сәйкестендіру және кіру құқықтарын басқару, VR класындағы қауіпсіздік, қауіпсіз байланыс және модерация, интеграция және API қорғау, криптографиялық деректерді қорғау, сондай-ақ бақылау және зерттеу инфрақұрылымы кіреді.

Ұсынылған модель нақты университет ортасында қауіпсіздіктің практикалық мүмкіндігін оны тізбектерге бөлу және айқын операциялық логика арқылы қамтамасыз етеді.

Алынған нәтижелердің практикалық маңыздылығы ұсынылған архитектура білім беру үшін қауіпсіз VR платформасын құрудың қайталанатын әдіснамасын анықтайды, ол бір уақытта мыналарды ескереді: (i) білім беру деректері мен байланыстарын қорғау, (ii) VR және чаттағы әлеуметтік-техникалық тәуекелдерді басқару, (iii) сәйкестік және процедуралық ашықтық талаптары. Болашақта зерттеуді одан әрі дамыту бейімделгіш оқыту сапасын сақтай отырып және жиналған сигналдарды азайта отырып, XR телеметриясын деанонизациялаудың қалдық тәуекелдерін ресми бағалауға және құпиялылықты сақтайтын аналитиканы (агрегация, дифференциалды құпиялылық, федеративті тәсілдер) масштабтауға бағытталуы керек. Құпиялылық пен байланыс қауіпсіздігі арасындағы тепе-теңдікке ерекше назар аудару қажет, әсіресе жақсартылған шифрлау және әділ модерация қажеттілігі аясында зиянды мазмұнды бақылау механизмдерін енгізу кезінде, бұл жергілікті деректер мен адамның циклдегі процедураларындағы модельдерді тексерудің маңыздылығын анықтайды.

**МҮДДЕЛЕР ҚАЙШЫЛЫҒЫ:** Автор мүдделер қайшылығы жоқ екенін мәлімдейді.

**ҚАРЖЫЛАНДЫРУ:** Бұл мақала AP23484442 бойынша Ғылым және жоғары білім министрлігінің ғылыми зерттеулерге арналған гранттық қаржыландыру жобасы аясында дайындалды.

**ИНСТИТУЦИОНАЛДЫҚ ЭТИКА КОМИТЕТІНІҢ ҚОРЫТЫНДЫСЫ:** Қолданылмайды.

**ЕРІКТІ КЕЛІСІМ ТУРАЛЫ МӘЛІМДЕМЕ**: Қолданылмайды.

**ДЕРЕКТЕРДІҢ ҚОЛЖЕТІМДІЛІГІ ТУРАЛЫ МӘЛІМДЕМЕ:** Осы зерттеудің нәтижелері негізінен сандық модельдеу мен теориялық талдауға сүйенеді. Жаңа эксперименттік деректер жиналмаған. Қажет болған жағдайда зерттеу нәтижелерін растайтын материалдар тиісті сұраныс бойынша жауапты автордан алынуы мүмкін.

**АЛҒЫС БІЛДІРУ:** Авторлар зерттеуді орындау барысында әдістемелік қолдау көрсеткен әріптестеріне және жұмыстың сапасын арттыруға ықпал еткен анонимді рецензенттерге алғыс білдіреді.

**ЖАСАНДЫ ИНТЕЛЛЕКТ ТЕХНОЛОГИЯЛАРЫН ПАЙДАЛАНУ ТУРАЛЫ ХАБАРЛАМА:** Авторлар бұл қолжазбаны дайындау кезінде генеративті жасанды интеллект құралдарын пайдаланбаған.

**ӘДЕБИЕТТЕР ТІЗІМІ**

Abedin, B., Meske, C., Junglas, I., & Osmundsen, K. (2022). Designing and managing human–AI interactions. Information Systems Frontiers, 24(3), 691–697. https://doi.org/10.1007/s10796-022-10313-1

Al-kaeed, M., Qayyum, A., & Qadir, J. (2024). Privacy preservation in Artificial Intelligence and Extended Reality (AI-XR) metaverses: A survey. Journal of Network and Computer Applications, 231, Article 103989. https://doi.org/10.1016/j.jnca.2024.103989

Alhloul, A., & Kiss, E. (2022). Industry 4.0 as a challenge for the skills and competencies of the labor force: A bibliometric review and a survey. Sci, 4(3), Article 34. https://doi.org/10.3390/sci4030034

Brehm, K., & Shvartzhnaider, Y. (2024). Understanding privacy in virtual reality classrooms: A contextual integrity perspective. IEEE Security & Privacy, 22(2), 62–69. https://doi.org/10.1109/MSEC.2023.3336802

Dutta, S., Lanvin, B., & Wunsch-Vincent, S. (Eds.). (2022). Global innovation index 2022: What is the future of innovation-driven growth? World Intellectual Property Organization. https://www.wipo.int/global_innovation_index/en/2022/

Garg, T., Masud, S., Suresh, T., & Chakraborty, T. (2023). Handling bias in toxic speech detection: A survey. ACM Computing Surveys, 56(3), Article 52. https://doi.org/10.1145/3580494

Giaretta, A. (2024). Security and privacy in virtual reality: A literature survey. Virtual Reality, 28(2), Article 79. https://doi.org/10.1007/s10055-024-01079-9

Laiz-Ibanez, H., Mendaña-Cuervo, C., & Carus Candas, J. L. (2025). The metaverse: Privacy and information security risks. Forensic Science International: Digital Investigation, 52, Article 100373. https://doi.org/10.1016/j.jjimei.2025.100373

Ren, X., Fan, J., Xu, N., Wang, S., Dong, C., & Wen, Z. (2024). DPGazeSynth: Enhancing eye-tracking virtual reality privacy with differentially private data synthesis. Information Sciences, 675, Article 120720. https://doi.org/10.1016/j.ins.2024.120720

Shen, Y., Wen, H., Luo, C., Xu, Y., Zhang, X., & Hu, J. (2019). GaitLock: Protect virtual and augmented reality headsets using gait. IEEE Transactions on Dependable and Secure Computing, 19(1), 418–432. https://doi.org/10.1109/TDSC.2019.2925774

Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2023). A survey on metaverse: Fundamentals, security, and privacy. IEEE Communications Surveys & Tutorials, 25(1), 319–352. https://doi.org/10.1109/COMST.2022.3202047

Wilson, E., Ibragimov, A., Proulx, M. J., Tetali, S. D., Butler, K., & Jain, E. (2024). Privacy-preserving gaze data streaming in immersive interactive virtual reality: Robustness and user experience. *IEEE Transactions on Visualization and Computer Graphics*, *30*(5), 2257-2268.

Zheng, T., Zhou, T., Lu, K., & Cai, Z. (2023). Inspecting end-to-end encrypted communication differentially for the efficient identification of harmful media. IEEE Transactions on Information Forensics and Security, 18, 4601–4615. https://doi.org/10.1109/TIFS.2023.3315067

Chen, H., Duan, H., Abdallah, M., Zhu, Y., Wen, Y., & Cai, W. (2023). Web3 metaverse: State-of-the-art and vision. ACM Transactions on Multimedia Computing, Communications, and Applications, 20(4), 1–42.

Microsoft. (n.d.). Minecraft Education [Computer software]. https://education.minecraft.net/

Roblox Corporation. (n.d.). Roblox Education [Virtual reality platform]. https://education.roblox.com/

ENGAGE XR Holdings. (n.d.). Engage VR [Virtual reality platform]. https://engagevr.io/

**Авторлар туралы мәліметтер**
**Информация об авторах**
**Information about authors**

**Ипалакова Мадина Тулегеновна** – қауымдастырылған профессор, инженерия ғылымдарының кандидаты, Халықаралық ақпараттық технологиялар университеті, Алматы, Қазақстан.
**Ипалакова Мадина Тулегеновна** – ассоциированный профессор, кандидат технических наук, Международный университет информационных технологий, Алматы, Казахстан.
**Ipalakova Madina** – Associate Professor, cand. of technical sciences, International Information Technology University, Almaty, Kazakhstan,
e-mail: m.ipalakova@edu.iitu.kz,
ORCID: https://orcid.org/0000-0002-8700-1852,

**Шарипов Данил Олегович** – Халықаралық ақпараттық технологиялар университетінің компьютерлік технологиялар және киберқауіпсіздік факультетінің ақпараттық технологиялар мамандығы бойынша бірінші курс магистранты, Алматы қ., Қазақстан
**Шарипов Данил Олегович** – магистрант 1 курса специальности «Информационные технологии» факультета Компьютерные технологии и кибербезопасность, Международный университет информационных технологий, г. Алматы, Казахстан
**Sharipov Danil** – first-year master's student in the Information Technology specialty, Faculty of Computer Technology and Cybersecurity, International University of Information Technology, Almaty, Kazakhstan
e-mail: 43760@iitu.edu.kz
ORCID: https://orcid.org/0009-0004-7780-6034

**Цой Дана Дмитриевна** – Инженерия ғылымдарының магистрі, Халықаралық ақпараттық технологиялар университетінің «Аралас шындық зертханасы» ғылыми-зерттеу зертханасының меңгерушісі, Алматы қ., Қазақстан
**Цой Дана Дмитриевна** – магистр технических наук, руководитель научно-исследовательской лаборатории «Лаборатория смешанной реальности» Международный университет информационных технологий, г. Алматы, Казахстан
**Tsoy Dana** – Master of Engineering Sciences, Head of the Research Laboratory "Mixed Reality Laboratory" International University of Information Technologies, Almaty, Kazakhstan
e-mail: d.tsoy@iitu.edu.kz
ORCID: https://orcid.org/0000-0003-0172-9760

**Дайнеко Евгения Александровна** – қауымдастырылған профессор, PhD, Автоматика және ақпараттық технологиялар институты, Сәтбаев университеті, Алматы қ., Қазақстан
**Дайнеко Евгения Александровна** – ассоциированный профессор, PhD, Институт автоматизации и информационных технологий, Сатпаев Университет, г. Алматы, Казахстан
**Daineko Yevgeniya** – Associate Professor, PhD, Institute of Automation and Information Technologies, Satpayev University, Almaty, Kazakhstan
e-mail: y.daineko@satbayev.university
ORCID: https://orcid.org/0000-0001-6581-2622

**Agariadne Dwinggo Samala** – Инженерлік факультетінің ассистенті, Негери Паданг университеті, Батыс Суматра, Паданг қ., Индонезия
**Agariadne Dwinggo Samala** – доцент инженерного факультета Университета Негери Паданг, Западная Суматра, г. Паданг, Индонезия
**Agariadne Dwinggo Samala** – Assistant Professor at the Faculty of Engineering, Universitas Negeri Padang, West Sumatra, Padang, Indonesia
Email: agariadne@ft.unp.ac.id
ORCID: https://orcid.org/0000-0002-4425-0605