

АҚПАРАТТЫҚ ҚАУІПСІЗДІК – ЦИФРЛЫҚ ҚОҒАМНЫҢ МАҢЫЗДЫ НЕГІЗІ

Қәдір Қ. Қ., экономика ғылымдарының магистрі, kkadir99@mail.ru

Қызылорда ашық университеті, Қызылорда қ., Қазақстан Республикасы

Аңдатпа. Қоғамның жедел цифрлануы, бұлттық сервистердің, мобильді қосымшалардың және жасанды интеллект құралдарының кең таралуы ақпараттық қауіпсіздікті жеке пайдаланушыдан бастап білім беру ұйымдары мен мемлекеттік құрылымдарға дейінгі барлық деңгейде өзекті мәселеге айналдырды. Зерттеудің мақсаты – қазіргі ақпараттық қауіптерді жүйелеу, олардың адам факторымен және білім беру ортасымен байланысын талдау, сондай-ақ қауіпсіздік мәдениетін қалыптастыруға бағытталған практикалық шараларды негіздеу. Зерттеу барысында Қазақстан Республикасының қолданыстағы нормативтік-құқықтық актілері, NIST Cybersecurity Framework 2.0, ENISA Threat Landscape 2025, Verizon 2026 DBIR материалдары және 2020–2026 жылдары жарияланған ғылыми еңбектерге салыстырмалы және контенттік талдау жүргізілді. Нәтижесінде ақпараттық қауіптердің техникалық, ұйымдастырушылық және мінез-құлықтық сипаттары бір-бірімен тығыз байланысты екені анықталды. Білім беру ұйымдары үшін басқару, техникалық қорғау, қолжетімділікті бақылау, резервтік қалпына келтіру және киберсауаттылықты біріктіретін бес компонентті тәсіл ұсынылды. Қорытындыда тұрақты оқыту мен тәжірибелік сценарийлер қауіпсіздік мәдениетінің маңызды бөлігі екені көрсетілді.

Түйінді сөздер: ақпараттық қауіпсіздік, киберқауіпсіздік, деректерді қорғау, фишинг, әлеуметтік инженерия, білім беру, цифрлық сауаттылық.

Аннотация. Быстрая цифровизация общества, широкое использование облачных сервисов, мобильных приложений и инструментов искусственного интеллекта сделали информационную безопасность актуальной задачей на всех уровнях – от отдельного пользователя до образовательных организаций и государственных структур. Цель исследования – систематизировать современные информационные угрозы, проанализировать их связь с человеческим фактором и образовательной средой, а также обосновать практические меры по формированию культуры безопасности. В работе применены сравнительный и контент-анализ действующих нормативных актов Республики Казахстан, NIST Cybersecurity Framework 2.0, ENISA Threat Landscape 2025, Verizon 2026 DBIR и научных публикаций 2020–2026 годов. Установлено, что технические, организационные и поведенческие причины киберрисков взаимосвязаны и требуют комплексного управления. Для образовательных организаций предложен пятикомпонентный подход, объединяющий управление, техническую защиту, контроль доступа, резервирование и восстановление, а также развитие киберграмотности. Сделан вывод о необходимости регулярного обучения пользователей и применения практических сценариев распознавания угроз.

Ключевые слова: информационная безопасность, кибербезопасность, защита данных, фишинг, социальная инженерия, образование, цифровая грамотность.

Кіріспе. Цифрлық технологиялар қазіргі қоғамның әлеуметтік және экономикалық инфрақұрылымының негізгі элементіне айналды. Электрондық құжат айналымы, қашықтан оқыту, мобильді банкинг, бұлттық сақтау жүйелері, әлеуметтік желілер және жасанды интеллект сервистері ақпаратты жинау, өңдеу және тарату жылдамдығын бірнеше есе арттырды. Сонымен бірге цифрлық ортаға тәуелділік өскен сайын деректердің жоғалуы, рұқсатсыз қол жеткізу, сервистің тоқтап қалуы және пайдаланушыны алдау арқылы құпия мәліметтерді иемдену тәуекелі де күшейеді. Қазақстандағы құқықтық база бұл мәселелерді киберқауіпсіздік, ақпараттық ресурстарды қорғау және дербес деректерді заңды өңдеу талаптары арқылы реттейді [1, 2].

Ақпараттық қауіпсіздік дәстүрлі түрде құпиялылық, тұтастық және қолжетімділік қағидаларымен түсіндіріледі. Құпиялылық ақпараттың тек уәкілетті тұлғаларға қолжетімді болуын, тұтастық ақпараттың рұқсатсыз өзгертілмеуін, ал қолжетімділік жүйелер мен деректердің қажет уақытта жұмыс істеуін білдіреді. Бұл үш қағида бүгін де өзекті болғанымен, қазіргі киберқауіпсіздік тек техникалық қорғаныс құралдарымен шектелмейді.

NIST Cybersecurity Framework 2.0 ұйымдарға кибертәуекелдерді басқаруды басқару, анықтау, қорғау, бақылау, әрекет ету және қалпына келтіру функциялары арқылы қарастыруды ұсынады [3]. Мұндай тәсіл ақпараттық қауіпсіздікті ұйымның жалпы басқару жүйесінің құрамдас бөлігі ретінде қабылдауға мүмкіндік береді.

Соңғы жылдардағы зерттеулерде адам факторы ерекше назарға алынуда. Pollini және әріптестері киберқауіпсіздікті тек технологиялық тұрғыдан қарастыру жеткіліксіз екенін, адамның мінез-құлқы, ұйым мәдениеті және жұмыс үдерістерінің өзара ықпалы тәуекел деңгейіне тікелей әсер ететінін көрсетеді [6]. Университет студенттерінің киберқауіпсіздік мінез-құлқын зерттеген Avcs мен Oguş ақпараттық қауіпсіздік туралы жалпы хабардарлық бар болғанымен, барлық студенттердің қауіпсіздік дағдылары бірдей қалыптаспағанын анықтаған [7]. Matyokurehwa және т.б. жоғары білім беру ұйымдарында әлеуметтік инженерия, зиянды бағдарламалар және интернет заттары саласындағы қауіптер жөніндегі хабардарлық деңгейінің оқу ортасына байланысты айырмашылықтары бар екенін көрсетеді [8].

Осы мәселенің өзектілігі білім беру ұйымдарында ерекше байқалады. Университеттерде студенттер мен оқытушылардың дербес деректері, бағалар, оқу материалдары, ғылыми нәтижелер, қаржылық және әкімшілік құжаттар сақталады. Сонымен бірге университет ортасында көптеген құрылғылар, жеке аккаунттар, ашық Wi-Fi, бұлттық платформалар және сыртқы сервистер қатар қолданылады. Бұл техникалық қорғаныс пен пайдаланушының қауіпсіз мінез-құлқын бір жүйеде қарастыруды қажет етеді. Зерттеудің мақсаты – қазіргі ақпараттық қауіптердің негізгі түрлерін жүйелеу, олардың білім беру ортасындағы ерекшелігін талдау және ақпараттық қауіпсіздік мәдениетін қалыптастырудың практикалық бағыттарын ұсыну.

Зерттеу материалдары мен әдістері. Зерттеу шолу-талдамалық сипатта жүргізілді. Материалдық база ретінде Қазақстан Республикасының ақпараттық қауіпсіздік пен дербес деректерді қорғау саласындағы қолданыстағы нормативтік актілері [1, 2], NIST Cybersecurity Framework 2.0 [3], ENISA Threat Landscape 2025 [4], Verizon 2026 Data Breach Investigations Report [5] және 2020-2026 жылдары жарияланған жоғары білім беру мен адам факторына қатысты ғылыми зерттеулер [6-10] алынды. Ғылыми еңбектерді іріктеуде үш өлшем қолданылды: зерттеудің ақпараттық немесе киберқауіпсіздікке тікелей қатыстылығы; пайдаланушы мінез-құлқы не білім беру ортасын қамтуы; нәтижелерінің практикалық ұсыныстар жасауға мүмкіндік беруі.

Негізгі әдістер ретінде салыстырмалы талдау, контенттік талдау, жіктеу және синтез қолданылды. Алдымен дереккөздерде жиі кездесетін қауіптер мен қорғаныс шаралары белгіленді; кейін олар техникалық, ұйымдастырушылық және адам факторына байланысты топтарға бөлінді. Екінші кезеңде халықаралық есептердің көрсеткіштері білім беру ұйымдарына тікелей көшірілмей, жалпы қауіп тенденцияларын сипаттайтын сыртқы контекст ретінде қарастырылды. Үшінші кезеңде ғылыми зерттеулердегі студенттердің хабардарлығы мен мінез-құлқына қатысты нәтижелер салыстырылып, білім беру ұйымдары үшін практикалық қауіпсіздік моделі қалыптастырылды.

Бұл жұмыста автор жүргізбеген сауалнама немесе эксперимент нәтижелері пайдаланылған жоқ. Сондықтан алынған қорытындылар эмпирикалық көрсеткіштердің жаңа жиынтығы емес, жарияланған зерттеулер мен ресми материалдарды жүйелеу нәтижесі болып табылады. Мұндай тәсіл зерттеудің шекарасын нақты көрсетуге және ұсыныстарды деректердің нақты қайнар көздеріне сүйене отырып қалыптастыруға мүмкіндік береді.

Нәтижелер және оларды талқылау. Жүргізілген талдау ақпараттық қауіпсіздіктің қазіргі мазмұнын үш өзара байланысты деңгей арқылы қарастыру орынды екенін көрсетті. Бірінші деңгей – техникалық қауіпсіздік: бағдарламалық осалдықтарды уақытында жою, құрылғыларды жаңарту, желіні қорғау, резервтік көшірме және зиянды кодтан қорғану. Екінші деңгей – ұйымдастырушылық қауіпсіздік: қолжетімділік құқықтарын бөлу, жауапкершілікті бекіту, оқиғаға әрекет ету тәртібі және тәуекелдерді басқару. Үшінші деңгей – адамның қауіпсіз мінез-құлқы: күрделі және бірегей парольдер қолдану, көпфакторлы

аутентификацияны қосу, күмәнді сілтемелер мен файлдарға сақтықпен қарау, дербес деректерді қажетсіз жарияламау және күмәнді жағдай туралы жауапты тұлғаға хабарлау. Бір деңгейдің әлсіздігі қалған қорғаныс тетіктерінің тиімділігін төмендетеді.

Қазіргі қауіп ландшафты бұл кешенділікті нақты көрсетеді. ENISA 2025 жылғы есебінде 2024 жылғы 1 шілде мен 2025 жылғы 30 маусым аралығындағы 4875 инцидент талданған; есепте фишинг бастапқы ену нүктелерінің 60%-ын, ал осалдықтарды пайдалану 21,3%-ын құрағаны көрсетіледі [4]. Бұл деректер Еуропалық Одақ кеңістігіне қатысты болғанымен, пайдаланушыны алдау мен техникалық осалдықтарды пайдалану қатар жүретінін дәлелдейтін маңызды жалпы тенденцияны көрсетеді. Verizon 2026 DBIR есебінде зерттелген деректер бұзылуларының 31%-ы бағдарламалық осалдықтардан басталғаны, ал 48%-ында ransomware қатысқаны көрсетілген [5]. Осы екі есептің нәтижесі «тек пайдаланушы қателеседі» немесе «тек техникалық жүйе әлсіз» деген біржақты түсіндірудің жеткіліксіз екенін көрсетеді.

Фишинг пен әлеуметтік инженерия білім беру ортасы үшін ерекше маңызды. Студент электрондық поштаны, мессенджерлерді, әлеуметтік желіні және оқу платформаларын бір мезетте қолданады; сондықтан шабуыл жасаушы оқытушының, университет әкімшілігінің, банк қызметкерінің немесе таныс адамның атын пайдаланып сенім тудыруы мүмкін. 2026 жылы жарияланған Ruzaili және әріптестерінің 202 студент қатысқан зерттеуінде алдын алу шаралары мен киберқауіпсіздік хабардарлығы арасында оң байланыс анықталған, бірақ фишинг туралы жай білімнің өзі қауіпсіз мінез-құлыққа автоматты түрде әкелмейтіні көрсетілген; қатысушылардың 27,2%-ы фишинг шабуылын бастан өткергенін хабарлаған [10]. Бұл нәтиже лекциялық түсіндіруді тәжірибелік тапсырмалармен толықтыру қажеттігін негіздейді.

Жоғары білімдегі басқа зерттеулер де осы тұжырымды қолдайды. Bottyan ақпараттық қауіпсіздік хабардарлығын білім беру ұйымының жалпы қорғаныс стратегиясының маңызды бөлігі ретінде қарастырады [9]. Matyokurehwa және т.б. студенттердің киберқауіпсіздік хабардарлығы білім деңгейі мен оқу орнына байланысты өзгеруі мүмкін екенін анықтаған [8]. Avcı мен Oguç зерттеуінде студенттердің жалпы хабардарлығы салыстырмалы жоғары болғанымен, қауіпсіз мінез-құлықтың жекелеген элементтерінде айырмашылықтар байқалған [7]. Демек, «студенттер интернетті жақсы қолданады, сондықтан қауіпсіздікті де жақсы біледі» деген болжам ғылыми тұрғыдан сенімді емес. Цифрлық дағды мен қауіпсіздік дағдысы өзара байланысты болғанымен, бір ұғым емес.

Жасанды интеллекттің жедел дамуы қауіптерді тағы бір деңгейге күрделендіреді. Генеративті жүйелер мәтін, дауыс және бейне контентін тез жасауға мүмкіндік бергендіктен, алаяқтық хабарламаларды жекелендіру, жалған нұсқаулық немесе сенімді көрінетін хат дайындау оңайлады. Verizon 2026 есебі генеративті жасанды интеллекттің әртүрлі шабуыл тәсілдерін күшейтіп отырғанын атап көрсетеді [5]. Сондықтан ақпараттың сыртқы көрінісіне ғана сену жеткіліксіз: пайдаланушы жіберушінің адресін, доменді, сұраудың мәнін және әрекеттің қалыпты жұмыс үдерісіне сәйкестігін тексеруі қажет. Білім беру барысында «ақпарат рас па?» деген сұрақпен қатар «осы хабарлама менен не істеуді талап етеді және бұл талап қауіпсіз бе?» деген талдау да қалыптасуы тиіс.

Қазақстан жағдайында ақпараттық қауіпсіздік мәдениетінің құқықтық бөлігі де маңызды. Қолданыстағы киберқауіпсіздік туралы заңнама ақпаратты қорғау құралдары мен цифрлық объектілер қауіпсіздігіне қойылатын талаптарды айқындайды [1]. «Дербес деректер және оларды қорғау туралы» заң дербес деректерді жинау, өңдеу және қорғау кезіндегі құқықтық негіздерді белгілейді және субъектінің құқықтарын қорғауды көздейді [2]. Университет үшін бұл талаптар тек IT бөлімінің міндеті емес. Дербес деректермен жұмыс істейтін оқытушы, деканат қызметкері, әкімшілік бөлім және ақпараттық жүйе пайдаланушысы өзінің рөлі шегіндегі қауіпсіздік талаптарын түсінуі тиіс.

Талдау нәтижесінде білім беру ұйымдары үшін ақпараттық қауіпсіздіктің бес компонентті моделі ұсынылады. Бірінші компонент – басқару және саясат: жауапты тұлғаларды, қолжетімділік ережелерін және инцидент туралы хабарлау тәртібін нақтылау.

Екінші компонент – техникалық қорғау: жаңарту, антивирустық және желілік қорғау, қауіпсіз конфигурация. Үшінші компонент – сәйкестендіру және қолжетімділік: бірегей парольдер, көпфакторлы аутентификация, рөлдік қолжетімділік және пайдаланушы құқықтарын мерзімді қайта қарау. Төртінші компонент – тұрақтылық: резервтік көшіру, журналдау, оқиғаны анықтау, әрекет ету және қалпына келтіру жоспары. Бесінші компонент – адам және білім: жүйелі оқыту, фишингті тану жаттығулары, нақты жағдайларды талдау және қауіпсіз цифрлық әдеттерді қалыптастыру. Бұл модель NIST-тің тәуекелдерді басқару логикасын [3] білім беру ортасындағы зерттеулермен [7-10] біріктіру арқылы ұсынылды.

1-кесте – Білім беру ұйымдары үшін негізгі ақпараттық қауіптер мен қарсы шаралар матрицасы

Қауіп тобы	Негізгі көрінісі	Ықтимал салдары	Басым қарсы шаралар
Фишинг және әлеуметтік инженерия	Жалған хат, мессенджердегі сілтеме, код немесе пароль сұрау	Аккаунттың бұзылуы, деректердің таралуы, қаржылық шығын	Практикалық оқыту; көпфакторлы аутентификация; жіберуші мен доменді тексеру
Бағдарламалық осалдықтар	Ескірген операциялық жүйе, қосымша немесе серверлік компонент	Рұқсатсыз кіру, зиянды кодтың орындалуы, қызметтің тоқтауы	Уақтылы жаңарту; осалдықтарды бақылау; қауіпсіз конфигурация
Ransomware және зиянды бағдарламалар	Файлдарды шифрлау, троян, шпиондық код	Деректердің қолжетімсіздігі, операциялық үзіліс, қалпына келтіру шығыны	Резервтік көшірме; сегментация; антивирустық қорғау; күмәнді файлдарды шектеу
Әлсіз аутентификация	Қайталанатын немесе қарапайым пароль, ортақ аккаунт	Бөгде тұлғаның жүйеге кіруі, әрекеттің авторын анықтай алмау	Бірегей пароль; MFA; рөлдік қолжетімділік; аккаунттарды мерзімді аудиттеу
Жасанды интеллектпен күшейтілген алдау	Сенімді мәтін, жалған дауыс/бейне, жекелендірілген хабарлама	Пайдаланушы сенімін теріс пайдалану, жалған тапсырманы орындау	Арна арқылы қайта растау; сұраудың контекстін тексеру; медиа және AI сауаттылығы

Ескерту – кесте автордың [3-10] дереккөздерін жүйелеуі негізінде құрастырылды.

Ұсынылған модельді іске асыруда оқыту формасының өзі маңызды. Қауіпсіздік туралы жылына бір рет жалпы нұсқаулық беру тұрақты мінез-құлық қалыптастыру үшін жеткіліксіз. Тиімді тәсіл – қысқа, бірақ жүйелі микросабактар, нақты сценарийлер және әрекет алгоритмдері. Мысалы, «банк атынан келген сілтемеге не істеу керек?», «Telegram немесе басқа мессенджердегі кіру кодын сұраса қалай әрекет ету қажет?», «оқытушының атымен келген файл күмәнді болса оны қалай тексеруге болады?» сияқты жағдайларды талдау пайдаланушыға қауіп белгісін тануды ғана емес, дұрыс жауап беру ретін де үйретеді. Ruzaili және т.б. зерттеуіндегі білім мен әрекет арасындағы алшақтық мұндай тәжірибелік бағыттың маңызын көрсетеді [10].

Ақпараттық қауіпсіздік мәдениетінің тағы бір шарты – пайдаланушыны тек «әлсіз буын» ретінде қабылдамау. Егер қауіпсіздік ережелері түсініксіз, жұмысқа кедергі келтіретін немесе шектен тыс күрделі болса, пайдаланушы оларды айналып өтуге тырысуы мүмкін. Сондықтан техникалық және ұйымдастырушылық шешімдер адамның нақты жұмыс үдерісіне бейімделуі тиіс. Pollini және әріптестері ұсынған адамға бағдарланған тәсіл осы ойды қолдайды [6]. Білім беру ұйымында қауіпсіздік саясаты жауапкершілікті күшейтумен қатар қауіп туралы хабарлауды жеңілдетуі, қателікті жасыруға емес, ерте хабарлауға ынталандыруы қажет.

Практикалық тұрғыдан университетте ең алдымен жоғары тәуекелді нүктелерді

анықтау орынды: әкімшілік және білім беру ақпараттық жүйелері, корпоративтік пошта, қашықтан оқыту платформалары, дербес деректер сақталатын файлдар, бухгалтерлік және кадрлық жүйелер. Әр нүкте бойынша кімнің қолжетімділігі бар, қандай мәлімет өңделеді, резервтік көшірме қайда сақталады және инцидент болғанда кімге хабарланатыны белгіленуі тиіс. Мұндай қарапайым инвентаризация күрделі құралсыз-ақ қауіпсіздік басқаруын тәртіпке келтіруге мүмкіндік береді және NIST CSF 2.0-дағы басқару мен тәуекелдерді анықтау қағидаларымен үйлеседі [3].

Сәйкестендіру мен қолжетімділікті басқару білім беру ұйымы үшін күнделікті қауіпсіздіктің өзегі болуы керек. Бір аккаунтты бірнеше адамның ортақ пайдалануы немесе қызметтік міндеті өзгергеннен кейін бұрынғы құқықтардың сақталып қалуы жауапкершілікті анықтауды қиындатады және қажетсіз тәуекел туғызады. Сондықтан пайдаланушыға тек өз міндетін орындауға қажетті құқықтарды беру, қызметтік рөлі өзгергенде қолжетімділікті қайта қарау, жұмыстан немесе оқудан кеткен аккаунттарды уақытында бұғаттау орынды. Құпиясөз жоғалған жағдайда көпфакторлы аутентификация қосымша қорғаныс қабатын береді. Бұл шаралар жеке бір техникалық құрал емес, қолжетімділік өмірлік циклін басқару қағидасы ретінде қолданылғанда тиімді болады.

Резервтік көшіру мен қалпына келтіру де тек көшірме жасаумен шектелмеуі тиіс. Ұйым көшірменің бар екенін ғана емес, одан деректі шынымен қалпына келтіруге болатынын мерзімді тексеруі қажет. Әсіресе оқу үдерісін, бағалау жүйесін, кадрлық және қаржылық қызметті қамтамасыз ететін деректер үшін қалпына келтірудің жауапты тұлғасы, басымдық реті және рұқсат етілетін үзіліс мерзімі алдын ала белгіленгені дұрыс. Мұндай дайындық ransomware немесе техникалық ақау кезінде шешім қабылдау уақытын қысқартады және қолжетімділік қағидасын нақты ұйымдастырушылық әрекетпен қамтамасыз етеді.

Қауіпсіздік мәдениетін бағалау үшін ұйым тек инцидент санын өлшем ретінде алмауы керек. Инцидент аз болуы кейде қауіптің аздығын емес, пайдаланушылардың оны хабарламауын білдіруі мүмкін. Сондықтан бақылау көрсеткіштері ретінде көпфакторлы аутентификациямен қорғалған аккаунттардың үлесі, жаңартуды орнату мерзімі, резервтік көшірмені қалпына келтіру сынақтарының нәтижесі, күмәнді хаттарды хабарлау саны, оқытуға қатысу деңгейі және анықталған оқиғаға алғашқы реакция уақыты сияқты көрсеткіштерді қолдануға болады. Бұл көрсеткіштер автор ұсынған бес компоненттің іске асу деңгейін жүйелі бағалауға мүмкіндік береді.

Білім беру мазмұны да мамандыққа қарай бейімделуі қажет. Ақпараттық технологиялар студенттері үшін желілік шабуылдар, осалдықтар және қауіпсіз бағдарламалау тақырыптарын тереңдету орынды болса, экономика, құқық, педагогика немесе басқа бағыт студенттеріне дербес деректер, фишинг, аккаунтты қорғау, құжат пен төлем деректерін қауіпсіз жіберу сияқты күнделікті сценарийлер маңыздырақ. Дегенмен барлық білім алушыға ортақ базалық минимум болуы керек: күмәнді сұрауды тану, құпия кодты бермеу, бірегей пароль қолдану, MFA қосу, бағдарламаны жаңарту және қауіп болғанда қайда хабарлау керегін білу. Осы минимум цифрлық сауаттылықтың практикалық бөлігі ретінде қалыптасуы тиіс.

2-кесте – Ұсынылған бес компонентті модельді іске асыру көрсеткіштері

Компонент	Ұйым деңгейіндегі әрекет	Бақылауға болатын көрсеткіш
Басқару және саясат	Жауапкершілік, ереже, инцидент туралы хабарлау арнасын бекіту	Құжаттардың өзектілігі; жауапты тұлғалардың анықталуы; хабарлау уақыты
Техникалық қорғау	Жаңарту, қауіпсіз конфигурация, зиянды кодтан және желілік қауіптен қорғау	Жаңартылмаған құрылғылар саны; анықталған осалдықтарды жабу мерзімі

Компонент	Ұйым деңгейіндегі әрекет	Бақылауға болатын көрсеткіш
Сәйкестендіру және қолжетімділік	MFA, рөлдік құқықтар, аккаунттардың өмірлік циклін басқару	MFA қамту үлесі; артық құқықтар саны; уақтылы бұғатталған аккаунттар
Тұрақтылық және қалпына келтіру	Резервтік көшіру, журналдау, оқиғаға әрекет ету және қалпына келтіру	Қалпына келтіру сынағының табыстылығы; реакция және қалпына келтіру уақыты
Адам және білім	Қысқа оқыту, фишинг сценарийлері, қауіпсіз цифрлық әдеттер	Оқытуға қатысу; күмәнді хаттарды хабарлау; практикалық тапсырма нәтижелері

Ескерту – көрсеткіштер автордың [3, 6-10] дереккөздерін талдау және білім беру ұйымдарының практикалық қажеттіліктерін жүйелеу негізінде ұсынылды.

Осылайша, зерттеу нәтижелері ақпараттық қауіпсіздіктің тиімді жүйесі үш шартқа сүйенетінін көрсетеді: технологияның сенімділігі, ұйымдық тәртіптің айқындығы және адамның қауіпсіз мінез-құлқы. Бұл үш шарттың біреуін елемеу қалған екеуінің әсерін әлсіретеді. Білім беру ұйымдары үшін ерекше міндет – студенттің кәсіби білімімен бірге қауіпсіз цифрлық мінез-құлқын да қалыптастыру. Өйткені бүгінгі студент ертең ұйымдардың ақпараттық ресурстарымен, клиенттердің деректерімен және цифрлық инфрақұрылыммен жұмыс істейтін маман болады.

Зерттеудің шектеулері. Зерттеудің негізгі шектеуі – жұмыста бір нақты университеттің ішкі статистикасы немесе автор жүргізген эмпирикалық сауалнама қолданылмағаны. Сондықтан халықаралық есептердегі көрсеткіштер Қазақстандағы білім беру ұйымдарының нақты деңгейін білдірмейді және жалпы қауіп тенденцияларын сипаттайтын салыстырмалы материал ретінде ғана пайдаланылды. Сонымен қатар әр елдегі құқықтық орта, цифрлық инфрақұрылым және пайдаланушы тәжірибесі әртүрлі болғандықтан, шетелдік зерттеулердің нәтижелері жергілікті ортаға тікелей көшірілмеуі керек.

Келесі кезеңде ұсынылған бес компонентті модельді Қызылорда өңіріндегі немесе нақты жоғары оқу орнындағы пайдаланушылар арасында тексеру зерттеудің қолданбалы құндылығын арттыра алады. Ол үшін анонимді сауалнама, қауіпсіз фишинг симуляциясы, оқытуға дейінгі және кейінгі білім деңгейін салыстыру, сондай-ақ резервтік қалпына келтіру мен инцидентке әрекет ету жаттығуларын бағалау әдістерін қолдануға болады.

Қорытынды. Зерттеу ақпараттық қауіпсіздіктің қазіргі цифрлық қоғамда тек техникалық мәселе емес, басқару, құқықтық реттеу және адамның мінез-құлқы бірігетін кешенді міндет екенін көрсетті. Құпиялылық, тұтастық және қолжетімділік қағидалары базалық негіз болып қала береді, бірақ қазіргі қауіп ортасында олар тәуекелдерді басқару, осалдықтарды уақтылы жою, инциденттерді анықтау және қалпына келтіру механизмдерімен толықтырылуы қажет.

Жұмыстың ғылыми-практикалық жаңалығы – халықаралық қауіп есептері, адам факторына арналған зерттеулер және білім беру ортасының ерекшеліктерін бір жүйеге біріктіріп, білім беру ұйымдары үшін бес компонентті модель ұсынуында. Модель басқару және саясатты, техникалық қорғауды, сәйкестендіру мен қолжетімділікті, тұрақтылық пен қалпына келтіруді, сондай-ақ киберсауаттылықты қамтиды. Оның басты қағидасы – қауіпсіздік шараларын бір-бірінен бөлек емес, өзара байланысты жүйе ретінде іске асыру.

Практикалық ұсыныс ретінде білім беру ұйымдарына ақпараттық активтер мен қолжетімділік құқықтарын тұрақты түгендеу, көпфакторлы аутентификацияны кең қолдану, резервтік көшірмені тексеру, бағдарламаларды уақытында жаңарту, инцидент туралы хабарлау тәртібін жеңілдету және студенттер мен қызметкерлерге қысқа тәжірибелік киберқауіпсіздік сабақтарын жүйелі өткізу ұсынылады. Болашақ зерттеулерде осы модельдің тиімділігін нақты университет базасында сауалнама, фишинг симуляциясы немесе оқу

алдындағы және оқудан кейінгі салыстырмалы бағалау арқылы эмпирикалық тексеру орынды.

Әдебиеттер тізімі:

1. Қазақстан Республикасының 2015 жылғы 24 қарашадағы № 418-V ҚПЗ «Киберқауіпсіздік туралы» Заңы (қолданыстағы редакция). – URL: <https://adilet.zan.kz/kaz/docs/Z1500000418> (қаралған күні: 22.09.2026).
2. Қазақстан Республикасының 2013 жылғы 21 мамырдағы № 94-V «Дербес деректер және оларды қорғау туралы» Заңы (қолданыстағы редакция). – URL: <https://adilet.zan.kz/kaz/docs/Z1300000094> (қаралған күні: 22.09.2026).
3. Pascoe C., Quinn S., Scarfone K. The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Papers, NIST CSWP 29. – 2024. – DOI: 10.6028/NIST.CSWP.29.
4. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2025. – Heraklion: ENISA, 2025. – URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025> (accessed: 22.09.2026).
5. Verizon. 2026 Data Breach Investigations Report. – 2026. – URL: <https://www.verizon.com/business/resources/reports/dbir/> (accessed: 22.09.2026).
6. Pollini, A., Callari, T.C., Tedeschi A., Ruscio D., Save L., Chiarugi F., Guerri D. Leveraging human factors in cybersecurity: an integrated methodological approach // Cognition, Technology & Work. – 2022. – Vol. 24. – P. 371–390. – DOI: 10.1007/s10111-021-00683-y.
7. Avcı Ü., Oruç O. Investigation of the Students' Personal Cyber Security Behaviour and Information Security Awareness // İnönü University Journal of the Faculty of Education. – 2020. – Vol. 21, No. 1. – P. 284–303. – DOI: 10.17679/inuefd.526390.
8. Matyokurehwa, K., Rudhumbu N., Gombero C., Mlambo C. Cybersecurity awareness in Zimbabwean universities: Perspectives from the students // Security and Privacy. – 2021. – Vol. 4, No. 2. – e141. – DOI: 10.1002/spy2.141.
9. Bottyan, L. Cybersecurity awareness among university students // Journal of Applied Technical and Educational Sciences. – 2023. – Vol. 13, No. 3. – Art. 363. – DOI: 10.24368/jates363.
10. Ruzaili, H., Katuk, N., Mohd Zaini, K., Abdullah W. Phishing awareness and preventive measures among university students: knowledge, behaviors, and victimisation perspectives // Millenium – Journal of Education, Technologies, and Health. – 2026. – Vol. 2, No. 29. – e43489. – DOI: 10.29352/mill0229.43489.