ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ

әл-Фараби атындағы Қазақ ұлттық университетінің

ХАБАРЛАРЫ

ИЗВЕСТИЯ

НАЦИОНАЛЬНОЙ АКАДЕМИИ
НАУК РЕСПУБЛИКИ КАЗАХСТАН
Казахский национальный
университет имени аль-Фараби

N E W S

OF THE ACADEMY OF SCIENCES
OF THE REPUBLIC OF
KAZAKHSTAN
al-Farabi Kazakh National University

SERIES
PHYSICO-MATHEMATICAL

3 (343)

JULY – SEPTEMBER 2022

PUBLISHED SINCE JANUARY 1963

PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

«ҚР ҰҒА Хабарлары. Физика-математикалық сериясы».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Меншіктеуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы қ.). Қазақстан Республикасының Ақпарат және қоғамдық даму министрлігінің Ақпарат комитетінде 14.02.2018 ж. берілген **No 16906-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік.
Тақырыптық бағыты: *ақпараттық коммуникациялық технологиялар сериясы.*
Қазіргі уақытта: *«ақпараттық технологиялар»бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*
Мерзімділігі: *жылына 4 рет.*
Тиражы: *300 дана.*
Редакцияның мекен-жайы: *050010, Алматы қ., Шевченко көш., 28, 219 бөл., тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Типографияның мекен-жайы: «Аруна» ЖК, Алматы қ., Мұратбаев көш., 75.

«Известия НАН РК. Серия физика-математическая».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Собственник: *Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы).*
Свидетельство о постановке на учет периодического печатного издания в Комитете информации Министерства информации и общественного развития Республики Казахстан **No 16906-Ж** выданное 14.02.2018 г.
Тематическая направленность: *серия информационные коммуникационные технологии.*
В настоящее время: *вошел в список журналов, рекомендованных ККСОН МОН РК по направлению «информационные коммуникационные технологии».*
Периодичность: *4 раз в год.*
Тираж: *300 экземпляров.*
Адрес редакции: *050010, г. Алматы, ул. Шевченко, 28, оф. 219, тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75.

News of the National Academy of Sciences of the Republic of Kazakhstan.

Physical-mathematical series.
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Owner: RPA «National Academy of Sciences of the Republic of Kazakhstan» (Almaty). The certificate of registration of a periodical printed publication in the Committee of information of the Ministry of Information and Social Development of the Republic of Kazakhstan **No. 16906-Ж,** issued 14.02.2018
Thematic scope: *series information technology.*
Currently: *included in the list of journals recommended by the CCSES MES RK in the direction of «information and communication technologies».*
Periodicity: *4 times a year.*
Circulation: *300 copies.*
Editorial address: *28, Shevchenko str., of. 219, Almaty, 050010, tel. 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Address of printing house: ST «Aruna», 75, Muratbayev str, Almaty.

NEWS OF THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 3, Number 343 (2022), 91-116
https://doi.org/10.32014/2022.2518-1726.141
УДК 004.056
МРНТИ 81.93.29

Ж.Д. Изтаев[1], Г.Т. Джусупбекова[1], Г.К. Ордабаева[2*]

[1]М. Әуезов атындағы Оңтүстік Қазақстан университеті,
Қазақстан, Шымкент;

[2]Әл-Фараби атындағы Қазақ ұлттық университеті, Қазақстан, Алматы.
E-mail: gulzi200988@mail.ru

УНИВЕРСИТЕТ ҮШІН АҚПАРАТТЫҚ ҚАУІПСІЗДІК ҚАТЕРЛЕРІНІҢ ЖЕКЕ МОДЕЛІН ӘЗІРЛЕУ

Аннотация. Бүгінгі таңда ақпараттық технологиялардың дамуымен есептеу және желілік қосымшалар университет ортасының ажырамас бөлігіне айналды. Қазіргі университеттер технологиялық прогрестің алдыңғы қатарында. Технологияға кең қолжетімділік құнды оқу орта-сына әкеледі, екінші жағынан, қауіпсіздікке қауіп төндіретін есептеу ортасының осалдығына әкелуі мүмкін. Университет кампустары Wi-Fi-ға кең қолдау көрсету, дәріс жазу бағдарламалық жасақтамасын қолдана отырып онлайн оқыту, сандық кітапхана, сыныптағы виртуализация, веб-конференциялар және т.б. сияқты мүмкіндіктерді ұсына отырып, әлемдегі технологиялық дамыған орындардың бірі ретінде өзін дәлел-деді.

Ашық үлкен кампусты үнемі өзгеріп отыратын қауіптер мен осалдықтардан қорғау өзекті мәселенің бірі. Университеттің ашық есептеу ортасының қолданушылары - студенттер, оқытушылар және әкімшілік. Университет кампусының желісі пайдаланушыларға қауіпсіз қол жетімділікті қамтамасыз етіп қана қоймай, оларды осалдықтардан да қорғауы керек. Әр қолданушы университеттік ресурстардың әр түрлі деңгейімен университеттік есептеу ортасына қол жеткізе алады. Кампустар желісінде тәуекел дәрежесін және қауіпсіздік тиімділігін арттыру қажет. Бұл өте маңызды қауіптерді анықтауды, кампус

желісін үздіксіз желілік бақылау арқылы тәуекел деңгейін өлшеу үшін осалдықтарды бағалауды талап етеді.

Мақалада әл-Фараби атындағы Қазақ ұлттық университетінің (ҚазҰУ) кампус желісінде болатын қауіпсіздік қатерлерін ескере отырып, университеттің есептеу ортасы үшін арнайы жасалған ақпараттық қауіпсіздік тәуекелдерін сандық бағалау моделі ұсынылған. Ұсынылған модель университет желісінің конфигурациясындағы ықтимал қауіптер мен ақпараттық процестерді анықтау арқылы қауіпсіздік тәуекелдерін сандық түрде өлшейді. Бұл модельді тәуекелдерді талдаушы және университеттің қауіпсіздік менеджері нақты және қол жетімді түрде сенімді және қайталанатын тәуекелдерді талдауды жүзеге асыру үшін қолдана алады.

Түйін сөздер: ақпараттық жүйелер, ақпараттық қауіпсіздік, модель, Nmap, Metasploit, Acunetix, мобильді қосымша.

Ж.Д. Изтаев[1], Г.Т. Джусупбекова[1], Г.К. Ордабаева[2*]

[1]Южно-Казахстанский университет им. М. Ауезова,
Казахстан, Шымкент;
[2]Казахский национальный университет имени аль-Фараби,
Казахстан, Алматы.
E-mail: gulzi200988@mail.ru

РАЗРАБОТКА ЧАСТНОЙ МОДЕЛИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ УНИВЕРСИТЕТА

Аннотация. Сегодня с развитием информационных технологий вычислительные и сетевые приложения стали неотъемлемой частью университетской среды. Современные университеты лидируют в технологическом прогрессе. Широкий доступ к технологии приводит к ценным средам обучения, с другой стороны, может привести к уязвимости вычислительной среды, угрожающей безопасности. Кампусы университета зарекомендовали себя как одно из технологически развитых мест в мире, предлагая такие возможности, как широкая поддержка Wi-Fi, онлайн-обучение с использованием лекционного программного обеспечения, цифровая библиотека, виртуализация в классе, веб-конференции и т.д.

Защита открытого большого кампуса от постоянно меняющихся угроз и уязвимостей является одной из актуальных проблем. Пользователи открытой вычислительной среды университета – студенты, преподаватели и администрация. Сеть кампуса университета должна обеспечивать не только безопасный доступ к пользователям, но и защищать их от уязвимостей. Каждый пользователь имеет доступ к университетской вычислительной среде с разным уровнем университетских ресурсов. Необходимо повысить степень риска и эффективность безопасности в сети кампусов. Это требует выявления очень важных рисков, оценки уязвимостей для измерения уровня риска путем непрерывного сетевого контроля сети кампусов.

В статье представлена модель количественной оценки рисков информационной безопасности, разработанная специально для вычислительной среды университета с учетом рисков безопасности в сети кампусов Казахского национального университета имени аль-Фараби (КазНУ). Предложенная модель количественно измеряет риски безопасности путем выявления возможных рисков и информационных процессов в конфигурации сети университета. Данная модель может применяться аналитиком рисков и менеджером по безопасности университета для осуществления анализа надежных и повторяющихся рисков в реальном и доступном виде.

Ключевые слова: информационные системы, информационная безопасность, модель, Nmap, Metasploit, Acunetix, мобильное приложение.

Zh.D. Iztayev[1], G.T. Dzhusupbekova[1], G.K. Ordabaeva[2*]

[1]South Kazakhstan University named after M. Auezov,
Kazakhstan, Shymkent;
[2]Al-Farabi Kazakh National University, Kazakhstan, Almaty.
E-mail: gulzi200988@mail.ru

DEVELOPMENT OF A PRIVATE MODEL OF INFORMATION SECURITY THREATS FOR THE UNIVERSITY

Abstract. Today, with the development of information technology, computing and networking applications have become an integral part of the university environment. Modern universities are leading the way in technological progress. Broad access to technology leads to valuable

learning environments, on the other hand, can lead to a security-threatening computing environment vulnerability. The university's campuses have established themselves as one of the technologically advanced places in the world, offering opportunities such as extensive Wi-Fi support, online learning using lecture software, digital library, classroom virtualization, web conferences, etc.

Protecting an open, large campus from ever-changing threats and vulnerabilities is one of the pressing challenges. Users of the open computing environment of the university are students, teachers and administration. The university's campus network should provide not only secure access to users, but also protect them from vulnerabilities. Each user has access to a university computing environment with a different level of university resources. It is necessary to increase the degree of risk and security efficiency in the network of campuses. This requires identifying very important risks, assessing vulnerabilities to measure the level of risk by continuously monitoring the network of campuses.

The article presents a model for quantitative assessment of information security risks, developed specifically for the computing environment of the university, taking into account security risks in the network of campuses of the Al-Farabi Kazakh National University (KazNU). The proposed model quantifies security risks by identifying possible risks and information processes in the configuration of the university network. This model can be used by a Risk Analyst and a University Security Manager to perform a real and available analysis of reliable and recurring risks.

Key words: information systems, information security, model, Nmap, Metasploit, Acunetix, mobile application.

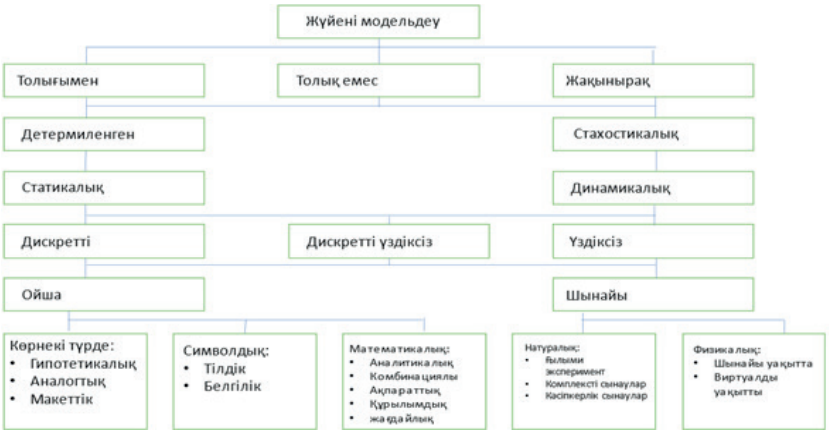
Кіріспе. Қазіргі заманғы типтік ақпараттық жүйелер (АЖ) – бұл клиент-серверлік аумақтық бөлінген көп қолданушы архитектурасы. Бағдарламалық жасақтама (әдетте қолданбалы бағдарламалық жасақтама) жалпы бағдарламалау тілдерін (мысалы, C#, TypeScript (бұрыштық даму платформасы, dotnet әзірлеу ортасы) қолдана отырып, ашық бағдарламалық интерфейске (API) негізделген функционалды модификацияларды ұсынады.

Жүйелерді модельдеу барлық ғылым салаларында басты зерттеу әдістерінің бірі және күрделі жүйелерді бағалаудың бірден-бір негізгі ғылыми әдісі. АЖ моделдеу - АЖ моделінің көмегімен түпнұсқа АЖ-нің маңызды қасиеттері туралы ақпарат алу мақсатында, нақты АЖ-ні басқасымен алмастыру түсініледі.

АЖ деректерді орталықтандырылған сақтау, жинақтау және бірнеше рет пайдалану қағидатын қамтамасыз етеді. Пайдаланушылардың автоматтандырылған жұмыс орындарында (АЖО) ресурстарды үнемдеу және ақпараттық қауіпсіздікті қамтамасыз ету үшін деректерді сақтау, өңдеу сервер көмегімен жүзеге асырылады.

АЖ жергілікті есептеу желісінен тыс орналасқан және АЖ серверлерімен ақпарат алмасуды жүзеге асыратын мобильді АЖО-да ақпаратты криптографиялық қорғау құралдары қолданылады.

Зерттеу әдістемесі мен материалдары. Жүйелерді модельдеу ұқсастық теориясына негізделген, оның негізгі мәні абсолютті ұқсастық тек бір объектіні басқасымен алмастыра алатын кезде ғана болуы мүмкін (1-сурет).



1-сурет. Жүйелерді модельдеу түрлерінің жіктелуі

Детерминленген модельдеу - кездейсоқ әсерлері жоқ процестерді көрсетеді. Стахостикалық модельдеу - ықтималды процестер және оқиғаларды көрсетеді. Статикалық модельдеу - АЖ-ның күйін кезкелген уақыт аралығында не болғанын сипаттайды. Динамикалық модельдеу - қазіргі уақыттағы АЖ-ның күйін көрсетеді. Дискретті модельдеу - АЖ-дағы дискретті, ал үздіксіз модельдеу - үздіксіз процестерді сипаттайды. Дискретті үздіксіз модельдеу - АЖ-дағы дискретті және үздіксіз процестерді сипаттауда қолданылады. Ойша модельдеу - шынайы объекттерді модельдегенде қолданылады, егер олар белгіленген уақыт аралығында қолжетімсіз болса немесе қолайсыз жағдайлар туындаса. Көрнекі модельдеу кезінде - АЖ-да болып жатқан құбылыстар мен процестерді бейнелейтін АЖ-ның көрнекі модельдері қалыптасады. Гипоткалық модельдеуде - нақты

АЖ-дағы процестердің заңдылықтары туралы гипотеза жасалады, ол сарапшының АЖ туралы білім деңгейін көрсетеді және зерттелетін АЖ-ның кірісі мен шығысының арасындағы себептік қатынастарға негізделген. Мұндай модельдеу АЖ құру үшін ақпараттар жеткіліксіз болған кезде қолданылады. Аналогтық модельдеу - әр деңгейдегі анаогтарды қолданады. Ең үздік деңгей зерттеліп отырған АЖ-ның толық аналогы болып табылады.

Математикалық модельдеу - нағыз АЖ модельіне қарап жасалынған математикалық модельдеу процесі. Аналитикалық модельдеу кезінде АЖ элементтерінің жұмыс істеу процестері кейбір функционалдық қатынастар (алгебралық, интегродифференциалды, айырмашылық және т.б.) немесе логикалық шарттар түрінде жазылады. Біріктірілген (аналитика - имитациялық) АЖ модельдеу екі модельдеудің жақсы жақтарын алады. Ішкі процестерге аналитикалық модель сәйкес келсе сол қолданылады, ал басқа кезде имитациялық модель қолданылады.

Физикалық модельдеу кезінде АЖ құбылыстардың табиғатын сақтайтын және физикалық ұқсастыққа ие жұмыс ортасында жүзеге асырылады. Физикалық модельдеу нақты және нақты емес уақыт шкаласында, сондай–ақ уақытты ескерусіз жүруі мүмкін.

Модельдерді құру әдістерінің жіктелуі 2 - суретте көрсетілген.

2 - сурет. Модельдерді құру әдістерінің жіктелуі

Бұл модельдердің негізгі кемшіліктері:

- модельдеу кезінде жаңа сапалық сипаттамаларды анықтау әрдайым мүмкін емес;

- кез-келген модель мүмкін құбылыстардың түсіндірілуін азайтады;
- статистикалық модельдер модель құрудың эмпирикалық жиынтығы аясында ғана объективті бола алады.

Мемлекеттік жалпыодақтық стандартта (государственный общесоюзный стандарт, ГОСТ, СТ РК ГОСТ Р ИСО/МЭК 15408-1-2006:52) ұғымдарды пайдалану мәнмәтінін және оларды қолдану тәсілін қоса алғанда, жалпы критерийлердің (ЖК) барлық бөліктерінде қолданылатын жалпы ұғымдар берілген. Қауіпсіздік активтерді қауіп-қатерден қорғаумен байланысты, онда қауіптер қорғалатын активтерді теріс пайдалану әлеуеті негізінде жіктеледі. Қауіптердің барлық түрлерін ескере отырып қауіпсіздік саласында адамның іс-әрекетіне, зиянды немесе басқа да байланысты мәселелерге көңіл бөлінеді.

Сонымен қатар, (СТ РК 1698-2007:33) «компьютерлік шабуыл - ақпаратқа, автоматтандырылған ақпараттық жүйенің ресурсына немесе бағдарламалық немесе бағдарламалық-аппараттық құралдарды қолдана отырып, оларға рұқсатсыз қол жеткізуге бағытталған рұқсатсыз әсер ету» деген анықтама берілген.

Қазіргі уақытта шабуылдардың көптеген модельдері, шабуылдарды модельдеу әдістері мен құралдары бар. Ақпараттық жүйелерге шабуылдардың негізгі модельдері 3 - суретте көрсетілген.

3 - сурет. Ақпараттық жүйелерге шабуыл модельдері

Шабуылдардың негізгі модельдерінің артықшылықтары мен кемшіліктері 1-кестеде келтірілген.

1-кесте. Шабуыл модельдерінің артықшылықтары мен кемшіліктері

№ р/н	Модель	Артықшылықтары	Кемшіліктері
1.	Кестелік (матрицалық)	Ең қарапайым	Циклдік шабуылдарды, оқыс оқиғалар немесе құқық бұзушының әрекеттері арасындағы көптеген байланыстарды модельдеу қиын.
2.	Логикалық	Инциденттерді өңдеу және пәндік сала туралы білімді ұсыну тілдерін қолдану. Модельдеу шабуылдары туралы белгісіздік жағдайларын ескереді.	Логикалық шығару механизмдерін қамтамасыз ететін қашықтықтан банктік қызмет көрсету (ҚБҚ) пайдалану;
3.	Графикалық	"Инциденттерді талдау, шабуылдарды анықтау, АҚ қамтамасыз ету үшін тәуекелдер мен ресурстарды барынша азайту" сияқты көптеген міндеттерді шешуге арналған	Элементтердің көптігі бар ақпаратты бағалау үшін графиктің пайда болуымен байланысты масштабталу.
4.	Шабуыл ағаштарындағы графтар	Көрнекілік, масштабталу, бейімделу, әмбебаптылық	Циклдік шабуылдарды модельдеу қиын; динамикалық модельдеудің болмауы
5.	Байес графтары	Көрнекілік, масштабталу, бейімделу, әмбебаптылық. шабуылдар туралы белгісіздік жағдайларын ескереді	Циклдік шабуылдарды модельдеу қиын; динамикалық модельдеудің болмауы
6.	Петри Желісі	Динамикалық және параллель процестерді модельдеудің ыңғайлылығы ықтималдық процестерді, уақыт параметрлерін қолдануды, зерттеу мен қолданудың қарапайымдылығын, көптеген көрсете алады.	Құқық бұзушының мінез-құлқы мен шабуылдың мақсаттарын сипаттай алмау
7.	Имитациялық	Құқық бұзушының мінез-құлық сипаттамаларын және шабуыл мақсаттарын модельдеуге мүмкіндік береді. Таратылған шабуылдарды модельдеу үшін ыңғайлы, көптеген құралдар бар және олар кең таралған	Үлкен есептеу ресурстарын қажет етеді

Шабуыл модельдерінің бірқатар кемшіліктері бар, атап айтқанда:

- модельдеудің күрделілігі;
- есептеу ресурстарын қажет етеді;
- ақпараттық қауіпсіздік (АҚ) саласындағы жоғары білікті мамандарды тартуды талап етеді;
- сараптамалық әдістердің қателіктері (сараптамалық бағалау).

Жүргізілген талдау негізінде қолданыстағы кемшіліктерді болдырмайтын өзекті ақпараттық қауіпсіздікті қорғауды (АҚҚ) анықтаудың жаңа әдістемелерін жетілдіру және әзірлеу қажеттілігі туралы қорытынды жасауға болады.

Khando (Khando et.al., 2021:22) ақпараттық қауіпсіздік саласындағы қызметкерлердің хабардар болуы (information security awareness, ISA) бойынша әдебиеттерге жүйелі шолу жасаған және жеке меншік ұйымдар мен мемлекеттік секторда қызметкерлерде ISA-ны арттыру үшін ISA әдістері мен факторларының заманауи жинағын ұсынады. Бұл зерттеу ISA контентін әзірлеу әдістері мен факторларындағы соңғы үрдістер туралы біраз түсінік береді, сондай-ақ ISA-ны өз ұйымдарында дамытудың жан-жақты бағдарламасын әзірлеуге көмектесу үшін ақпараттық қауіпсіздік жөніндегі мамандар арасында ақпарат пен білімді тарату жолымен ISA озық тәжірибесін енгізуге ықпал етеді.

У.А. Төкеев (Төкеев т.б., 2011:161) ақпараттық қауіпсіздік қатерін бағалау мен анализдеу әдістерін дамытуда айтарлықтай үлес қосқан отандық ғалымдар. Берілген оқу құралы ақпараттар қауіпсіздігін басқару жағынан мемлекеттік тілде жазылған алғашқы оқу-әдістемелік нұсқаулық. Оқу құралы 7 тараудан және біренше қосымшалардан тұрады. Әр тараудан соң шағын жаттығулар мен есептер берілген.

Ахметов Б.С. (Ахметов т.б., 2015:8) зерттеулерінде ұлттық және халықаралық құжаттарда ашылып отырған қауіп түсінігінің анализіне талдау жасалған. Ақпараттық қауіпсіздік саласында көптеген түсініктер ішінен қауіптің базалық сипаттамасы анықталған. Сонымен бірге, ақпараттық қауіпсіздік саласындағы бейнеде қауіптің базалық сипаттамасын п-компоненттік кортежді моделі түрінде таныстыру ұсынылған. Мақалада ақпараттық қауіпсіздік саласындағы кезекті талдау жасау үшін қауіп түсінігі ашылған және оның базалық сипаттамасы анықталған. Бұл ақпаратты қорғау тапсырмаларын тиімді шешуді жоғарылату мүмкіндігін кеңейтеді.

М.Н. Калимолдаев (Калимолдаев т.б., 2017:7) математикалық логиканы пайдалана отырып ақпараттық ресурстарға қолданушылардың қол жетімділік құқықтары мен мүмкіндіктерінің моделін қарастырған.

Логикалық жүйе түрінде қолжетімділікті типтелген атрибуттық шектеу моделін ұсыну субъектілердің объектілерге қауіпсіз қол жеткізуін қамтамасыз ете отырып, мәндерге артықшылықтар берудің дұрыстығын және жүйе жұмысының дұрыстығын формальды түрде дәлелдеуге мүмкіндік береді. Сонымен қатар, логика түріндегі қолжетімділікті типтелген атрибуттық ажырату моделі логикалық және функционалдық бағдарламалау тілдерінде тікелей іске асырылады.

Akhmetov B. зерттеулерінде (Akhmetov et.all., 2015:9) ірі оқу орындарының, атап айтқанда, Иордания, Қазақстан және Украина университеттерінің киберқауіпсіздік жүйелерінде өзара инвестициялық бақылау стратегияларының ұтымды нұсқаларын іздеу моделі қарастырылған. Мақала киберқауіпсіздік жүйелерінің инвестициялық параметрлері мен біздің мемлекеттің ірі білім беру мекемелерінің ақпараттық-білім беру ортасын қорғауға байланысты басқа да міндеттерді қамтамасыз ету арасындағы әртүрлі өзара байланыстарға арналған. Ғылыми зерттеулердің осы сегментегі басқа авторлардың жұмыстарына қарағанда өзгешілігі, өзара инвестициялар процесіндегі нақты параметрлер мен ұсынымдарды айқындау қабілеттігі. Сондықтан Иордания, Қазақстан және Украина жоғары оқу орындарының үлгісінде ақпараттық-білім беру платформаларында және оқу орындарының киберқауіпсіздігіндегі басқарушылық шешімдерді оңтайландыру үшін алғышарттар жасалған.

Khairur Razikin (Khairur Razikin et.al., 2022:22) ISO/IEC 27001 киберқауіпсіздік құрылымы негізінде ақпараттық технологиялар қауіпсіздігі жүйесін құру кезінде киберқауіпсіздік саласында шешімдер қабылдауды әзірлеуге арналған модель зерттелген. Ұсынылып отырған модель қауіп-қатерлерді жеңілдету үшін ең үздік қауіпсіздік жүйесін алуға бағытталған. Бұл құжат ақпараттық технологиялар қауіпсіздігі жүйелерін әзірлеу кезінде ең жақсы қадамдарды айқындау үшін киберқауіпсіздік саласында шешімдер қабылдауды қолдау жөніндегі ұсынымдарды әзірлеуде стратегиялық директивті органдарға ықпал етті.

Лахно В. (Лахно и др., 2021:11) өз зерттеулерінде кибершабуылды анықтау кезінде ақпараттық-коммуникациялық желілеріне кіру қаупі мен кезеңдерін болжау барысында шешімдер қабылдауды қолдау жүйесінің есептеу ядросы үшін байесовтік желілердің (БС) үлгілерін әзірлеген. Ұсынылған БС үлгілері көптеген кездейсоқ айнымалыларды операцияға және берілген шарттар кезінде кибернетикалық қатерді немесе кіру нақты кезеңін іске асыру ықтималдығын анықтауға

мүмкіндік береді. Байестің динамикалық желілерін (DSB) қолдану негізінде желілік басып кірулерді анықтаудың ықтимал модельдерімен толықтырылған. Әзірленген модельдердің тиімділігі бұрын оқытуда қолданылмаған тестілік негізде тексерілген.

Барабанов А.В. (Барабанов, и др., 2017:224) оқу құралында ұйымдарда ақпаратты көп деңгейлі қорғау кезінде қолданылатын базалық қағидаттар, тұжырымдамалық тәсілдер мен ақпараттық технологиялар баяндалған. Компьютерлік жүйелердің ақпараттық ресурстарының қауіпсіздігін қамтамасыз ету әдістері, желілік қауіпсіздік, техникалар мен құралдарды құрылымдау және жіктеу жолдары терең баяндалған.

Лившиц И.И. (Лившиц и др., 2018:407) ғылыми жұмысында қазіргі заманғы кешенді тәуекел-бағдарланған тәсілге, ақпараттық қауіпсіздік менеджменті жүйесінде ақпараттық қауіпсіздік аудитін (АҚА) орындаудың арнайы модельдері мен әдістеріне негізделген өнеркәсіптік объектілер үшін ақпараттық қауіпсіздік аудитін қамтамасыз етуге арналған ғылыми-әдістемелік аппарат қалыптастырылған. Модельдер мен әдістер кешенінің жаңалығы АҚА орындау үшін функционалдық аяқталған құрылымды қалыптастыру болып табылады.

Jaafer Al-Saraireh (Jaafer Al-Saraireh, et al., 2022:11) зерттеу жұмысында кеңейтілген тұрақты қатер (Advanced Persistent Threat, APT) шабуылдарының деректер жиынтығын пайдалана отырып, APT шабуылдарын анықтау тәсілі ұсынылған. Деректер жиыны түрлі шабуылдар түрлерінің негізінде APT шабуылдарын анықтау үшін ұсынылған машиналық оқыту (ML) моделіне орналастырылды. Деректердің бес түрі жиналды, атап айтқанда, қалыпты, рекогносцирлік, бастапқы ымыраға келу, бүйірлік қозғалыс және деректерді сүзгілеу. Деректердің әрбір түрі қаскүнем өтуі мүмкін кезеңді көрсетеді. Көрнекті өнімділікке деректер жиынтығындағы 65 функцияның тек 12 функциясын пайдалана отырып, 99,89% дәлдікпен қол жеткізілді.

Зерттеу нәтижелері. Бағдарламалық жасақтаманы автоматтандырылған өңдеу және әзірлеу үшін мәліметтер жиынтығын ұсыну мақсатында Python 3 бағдарламалау тілі және Data Science технологиясы қолданылды.

Деректерді автоматтандырылған өңдеуді дайындау үшін деректерді түрлендіру қажет. Деректерді түрлендіруге арналған Python 3 бағдарламалау тіліндегі код 4-суретте келтірілген:

```
train = pd.read_csv('threats.csv', encoding='utf-8')
df = pd.get_dummies(train)
# Жол деректерін түрлендіру
for col in list(df.columns):
if ('ft²' in col or 'kBtu' in col or 'Metric Tons CO2e' in col or 'kWh' in
col or 'therms' in col or 'gal' in col or 'Score' in col):
# Конвертация
df[col] = df[col].astype(float)
```

4-сурет. Python 3 бағдарламалау тілінде деректерді түрлендіру

Тәуекелдерді бағалаудың көптеген модельдері бар, алайда, ұйымдарға ұйым ішінде қай модельді қолдануға болатындығын анықтауға көмектесетін механизм жоқ. Сонымен қатар, бұл модельдер банктер сияқты мақсатты ұйымдарды бұзу кезінде анықталған қауіпсіздік мәселелерін ескереді. Қауіпсіздік тәуекелдерін бағалау бұл ұйымдар үшін өте маңызды болғанымен, біріншіден, ұйымдар қауіпсіз және жабық желілік ортаға ие. Екіншіден, ақпараттық қауіпсіздік тәуекелдерін бағалау негізгі және басым міндет болып табылатын университеттер сияқты жоғары оқу орындарында үлкен және ашық есептеу ортасы бар. Университеттің үлкен есептеу ортасына әртүрлі желілік құрылғылар, бағдарламалық қосымшалар және көптеген серверлер кіреді. Ұсынылған модельдің маңыздылығы мен тиімділігін бағалау үшін ҚазҰУ -нің есептеу ортасы қолданылды (5-сурет).

5-сурет. ҚазҰУ университетінің есептеу ортасы үшін желіні орнату

Ақпараттық қауіпсіздік тәуекелдерін басқарудың ұсынылып отырған құрылымы тәуекелдерді басқарудың үздіксіз процесін айқындайды, әр түрлі әрекеттер тізбегінен тұрады. Ұсынылған модельдің бірін-

ші кезеңінде ұйымның ақпараттық активтерінің тәуекелдеріне толық талдау жасалады және нәтижелер негізінде келесі әрекеттер анықталады: бірінші кезеңдегі іс-әрекеттің мақсаты - осалдық сканері немесе ену тесті сияқты әртүрлі көздерден университеттің есептеу ортасында көрінетін және қолдануға болатын әлсіздіктер мен осалдықтарды анықтау. Бірінші кезеңнің нәтижелері екінші кезеңдегі тәуекелдерді талдауда қолданылады, келесі қадамда барлық активтер үшін тәуекелдерді бағалау жүргізіледі.

Бірінші кезеңде кампус желісінің қауіпсіздігін қамтамасыз етуге ұсынылған тәсіл ақпаратты маңызды активтердің бірі ретінде анықталады. Университеттің есептеу ортасы үшін қауіпсіз инфрақұрылымды дамыту қауіпсіздік мамандары байланыс инфрақұрылымының бөлігі бола алатын техникалық активтерге (желіге қосылу кабельдері, маршрутизаторлар мен коммутаторлар) немесе құрылғы инфрақұрылымына (физикалық немесе виртуалды хосттар) назар аударады және бағдарламалық жасақтама болуы мүмкін.

Университеттің есептеу жүйесінің сипаттамасы есептеу жүйесінің шектеулерін, сондай-ақ желілік ортаны құрайтын ресурстар мен ақпаратты анықтау арқылы тәуекелді бағалауға күш салады. ҚазҰУ университеті кампусының үлкен және ашық желілік ортасы негізінен келесі қауіпсіздік қатерлеріне ұшырайды - Фишинг, Ransomware және зиянды бағдарламалар. Киберқылмыскерлер қаржылық пайда алу үшін ресми хабарламаларды бұрмалайтын электрондық пошталарды немесе веб-шоттарды пайдаланады. Университеттің жас студенттері көбінесе фишингтік шабуылдардың құрбаны болады, нәтижесінде зиянды бағдарламалар немесе бопсалау бағдарламалары жүктеледі.

ҚазҰУ қалашығының аумағында Wi-Fi-ға қол жетімділік қамтамасыз етіледі, бұл техникалық прогресс тұрғысынан өте жақсы, бірақ күтпеген жерден қауіпсіздік мәселелерін тудыруы мүмкін.

Университет жастары Facebook, Telegram және YouTube сияқты әлеуметтік желілердің ең белсенді қолданушылары болып табылады. Бұл университет желісінде зиянды бағдарлама әлеуметтік медиа көмегімен таралуы мүмкін дегенді білдіреді.

Көптеген мобильді құрылғылар негізінде қауіп-қатер де көп. Студенттер технологияны бірінші болып игереді және кампуста жаңа құрылғылар жиі пайда болады - iPad–тан бастап жаңа Android телефондары.

Осалдықтарды анықтау және бағалау мақсатында келесі желіні сканерлеу қосымшалары қолданылды: Nmap, Nexpose және Acunetix.

Сагар Рахалкар Пуна (Сагар Рахалкар Пуна, 2019:144) ақпараттық қауіпсіздіктің саласындағы 11 жылдық тәжірибесі бар маман. Ол киберқылмыстарды тергеуге, цифрлық криминалистикаға, қосымшалардың қауіпсіздігіне, осалдықты бағалауға және енуге тестілеуге, мандаттар мен нормативтік актілерді сақтауға маманданған. Бұл оқулықта NMAP, OpenVAS және Metasploit сияқты үш құралдың негіздерімен танысасыз және осы үш құралды пайдалана отырып, ену үшін тестілеудің кең мүмкіндіктеріне ие боласыз.

Ордабаева Г.К. (Ордабаева, 2020:6) зерттеуінде OSI моделінің физикалық, арналық және желілік деңгейіндегі таратылған есептеу жүйесі объектілерінің өзара әрекеттесуін сипаттайтын бағытталған графты қолдана отырып жасалған ақпараттық жүйенің моделі берілген. Қолданылуы қарапайым Nessus Vulnerability Scanner негізінде желінің осалдығын анықтау әдісі келтірілді. Nessus Vulnerability Scanner осалдықты анықтаудағы үздік сканер болып табылады. Басты артықшылығы – деректер базасындағы қауіпті моделдер негізінде желіні тез әрі сапалы тексереді.

Eric Filiol (Eric Filiol, et al., 2021:8) зерттеуінде Red Hat хакерлері орындайтын осалдықты анықтау және жою процесін автоматтандыруға бағытталған әдіс ұсынылған. Ұсынылған әдіс Metaesploitable Linux дистрибутивін пайдалана отырып бағаланған. Нәтижеде кең таралған алты сервиске назар аударылған: ftp, ssh, telnet, rdp, StartViewer және Printer. Ұсынылған әдіс кең таралған осалдықтарды автоматты түрде жоюға қабілетті екені көрсетілген.

Университет ортасында қауіпсіздіктің ықтимал қауіптерін анықтағаннан кейін, келесі қадам–сәтті шабуыл нәтижесінде шығындардың ықтимал әсерін анықтайтын осалдықты бағалау. Осалдықтарды сканерлеу әкімшіге желідегі қауіпсіздіктің нақты жағдайы туралы хабарлайды және шабуылдаушы кез–келген осалдықты бірінші болып тапқанға дейін түзетуді анықтауға көмектеседі. Университет желісі үлкен және ашық, сондықтан бүкіл желіні сканерлеудің орнына біз хосттарды топтарға жіктеп, әр топты сканерлейміз.

Сканерлеу мақсаты – жүйенің конфигурациялары туралы егжей-тегжейлі түсінік алу үшін сыртқы қауіпсіздікке қарсы шараларды болдырмау. Сканерлеу қауіпсіздік жағдайын анықтауға арналған, яғни, егер ҚазҰУ университетінің желісін зерттеуге тырысса, хакердің не көретінін анықтау. ҚазҰУ университетін сканерлеу үшін Nmap, Nexpose, Metasploit және Acunetix сияқты құралдар пайдаланылды. Nmap және Nexpose құралы осалдықтар үшін сканерленуі керек

желідегі хосттарды іздеу үшін, Acunetix веб-осалдықтарды сканерлеу үшін, ал Metasploit Nexpose-пен бірге енуді тестілеу үшін қолданылады.

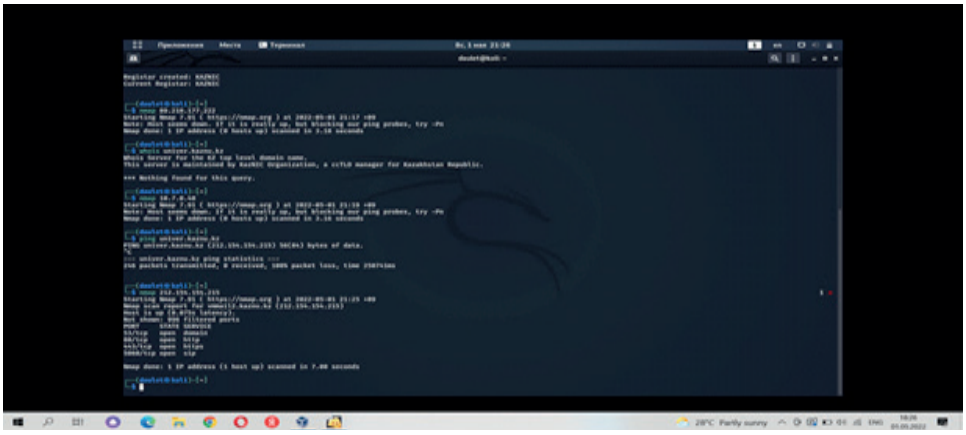
Nmap (Network Mapper) – желіні және қауіпсіздік аудитін анықтауға арналған ақысыз, ашық көзі бар желілік сканерлеу құралдарының бірі. Nmap міндеттері: хосттарды анықтау және портты сканерлеу.

Nmap және Nexpose желідегі хосттар мен қызметтерді іздеу үшін университеттің маршрутизатор аймағында орналасқан. Осы уақытта Nexpose 996 қызметі бар 5 хостты тапты, олардың ішінде университеттің негізгі сервері 27 жоғары, 15 орташа және 9 төмен осалдықпен жұмыс істейді. 2-кестеде Nexpose жасаған нәтижелер, хосттар туралы кейбір мәліметтер берілген.

2-кесте. Nexpose қосымшасымен анықталған хосттар

Табылған	IP	Хост атауы	Операциялық жүйелер	Қызметтер
19.04.22 17:31	212.154.154.215	univer.kaznu.kz	Белгісіз	465
19.04.22 17:31	212.154.154.215	ИКС	Windows 10	7
19.04.22 00:44	212.154.154.215	212.154.154.215	Linux	4

TCP қосылымын (–sT) сканерлеу белсенді хостты анықтау үшін Nmap қосымшасы арқылы жүзеге асырылады. Берілген уақыт белгісінде Nmap 996 портты сканерледі, соның ішінде ашық түрде анықталған порттар 6- суретте берілген.



6-сурет. Nmap қосымшасымен ашық порттарды анықтау

Ашық порттың күйі шабуылдаушының осы порттарды қолдана отырып желіге кіре алатындығын көрсетеді. Бағдарлама TCP қосылымдарын, UDP датаграммаларын белсенді қабылдайды. Қауіпсіздік

қызметкерлері әрбір ашық порт шабуылдың жолы екенін біледі. Зиянкестік әрекеттер ашық порттар көмегімен орындалады, ал желілік әкімші міндеті осы порттарды брандмауэрмен жабу және қорғау.

Порттарды қарап шығу кіру нүктелеріне әкеледі, олар арқылы зиянкестер желіге кіре алады. Біздің желідегі әлсіздіктерді жою үшін қауіпсіздік мамандары біздің желідегі осы осалдықтар туралы білуі керек. Nmap және Nessus осалдық сканерлері ҚазҰУ университетінің есептеу ортасында болатын желілік осалдықтар туралы ақпаратты анықтау үшін қолданылады. 7-суретте Nmap көмегімен осалдықты анықтау нәтижесі берілген. Портты сканерлеу нәтижесі 445 портының 208.91.199.121 хостында ашылғанын көрсетеді. 445 порт - бұл TCP порты, ол сервердің хабарлама блогының (SMB) осалдығына ұшырауы мүмкін. Осалдықты тексеру үшін Nmap SMB-vuln-ms08067 сценарийі іске қосылады.

```
root:~# nmap -p 445  212.154.154.213-script=smb-vuln-ms08-067.nse

Starting Nmap 7.40 ( https://nmap.org ) at 2022-04-25 10:56 IST
Nmap scan report for 192.168.1.212
Host is up (0.00050s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:25:C3:51

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250

Nmap done: 1 IP_address (1 host up) scanned in 7.08 seconds
```

7 - сурет. Metasploit енуге тестілеу нәтижесі

Сканерлеу нәтижесі хосттың MS08-067 деп аталатын кодты қашықтан орындау осалдығына ұшырайтындығын көрсетеді. Бұл тексеру қауіпті және жүйенің бұзылуына әкелуі мүмкін. Ұйымның қауіпсіздік қызметкерлері үшін мұндай тексерулерді жүргізу өте маңызды, өйткені бұл осалдықты пайдалана отырып жүйеге көптеген зияндық келтіруі мүмкін.

Біз өз зерттеуімізде Metasploit-ты осалдықтарды бағалау үшін енуге тестілеу құралы ретінде пайдаланамыз. 8 - суретте Metasploit ену тестілеу нәтижесі көрсетілген.

```
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   RHOST     212.154.154.213  yes       The target address
   RPORT     445              yes       The SMB service port (TCP)
   SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting

msf exploit(ms08_067_netapi) > check
[+] 192.168.1.212:445 The target is vulnerable.
msf exploit(ms08_067_netapi) >
```

8-сурет. Metasploit қосымшасымен енуді тестілеу нәтижесі

Nmap және Nessus осалдықтарын сканерлеп, Metasploit ену тестінен кейін біз ҚазҰУ университетінің желілік ортасында болатын кейбір маңызды осалдықтарды таптық. Маңызды осалдықтар жылдам әрекет етуді талап етеді, өйткені шабуылдаушыға оларды пайдалану оңай және олар жүйені толық бақылауға мүмкіндік береді.

Веб-қосымшалар мен веб-қызметтер университеттің есептеу ортасының негізгі құрамдас бөлігі болып табылады. Алайда, веб-сайттар мен веб-қосымшаларда құпия корпоративтік деректердің, несие карталарының, тұтынушы туралы ақпараттың және жеке басын анықтайтын ақпараттың ұрлануына әкелуі мүмкін осалдықтар бар.

Ұйымның қауіпсіздік деңгейін жоғарылату үшін веб-қосымшалардың қауіпсіздігін тек басымдыққа ғана емес, сонымен қатар негізгі талап ретінде қарастыру керек. Осы бағытта веб-сканерлеу ҚазҰУ университетінің веб-серверіне арналған Acunetix веб–сканерінің көмегімен орындалды (9- сурет).

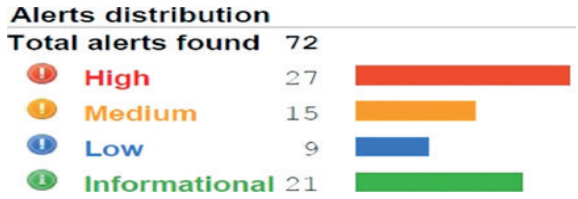
Alerts (72) Knowledge Base (4) 27 15 9 21 Generate Report

Start Date	19 Apr 2022 21:40	Files	15	Requests	17287	Host Name	http://univer.kaznu.kz
End Date	19 Apr 2022 21:40	Directories	6	Avg. Response Time	142.78 ms	Scan Target Name	Univer Kaznu Web Scan
Duration	7h 56m 5s	Variations	14	Responsive	Yes	Scan Type	Web

	Name	Module
+	Blind SQL Injection (6)	Scripting (Blind_Sql_Injection.script)
+	Cross site scripting (verified) (1)	Scripting (XSS.script)
+	Directory traversal (1)	Scripting (Directory_Traversal.script)
+	Microsoft IIS tilde directory enumeration (1)	Scripting (IIS_Tilde_Dir_Enumeration.script)
+	Script source code disclosure (1)	Scripting (Script_Source_Code_Disclosure.script)
+	SQL injection (verified) (15)	Scripting (Sql_Injection.script)
+	Weak password (2)	Scripting (Html_Authentication_Audit.script)
+	Application error message (10)	Scripting (Error_Message.script)
+	HTML form without CSRF protection (3)	Crawler
+	User credentials are sent in clear text (2)	Crawler
+	ASP.NET version disclosure (1)	Scripting (ASP_NET_Error_Message.script)
+	Clickjacking: X-Frame-Options header missing (1)	Scripting (Clickjacking_X_Frame_Options.script)
+	Cookie without HttpOnly flag set (1)	Crawler
+	Cookie without Secure flag set (1)	Crawler
+	Login page password-guessing attack (4)	Scripting (Html_Authentication_Audit.script)

9-сурет. Acunetix веб-сканерлеу нәтижесі

10 - суретте анықталған хост ескертулері жинақталған сыртқы сканерлеу нәтижесі берілген.



10-сурет. Acunetix қосымшасымен 212.154.154.213 хостты веб-сканерлеу нәтижесі

Тәуекелді бағалау үшін ықтималдық, статистика және ақпараттық технологияларды білетін білікті мамандар қажет. Тәуекелдерді өлшеудің алғашқы қадамы әртүрлі сканерлерден, атап айтқанда, Nexpose, Acunetix және Metasploit–тен алынған барлық сканерлеу нәтижелерін орталықтандыруды қажет етеді (3-кесте).

3-кесте. Интеграцияланған сканерлеу нәтижелері

Осалдық	Қатаңдық	Барлық ескертулер	Категория
Әлсіз пароль	7,5	2	Қатыгез шабуыл
Әлсіз пароль	7,5	2	Аутентификацияның жеткіліксіздігі
Сайт аралық скриптинг (тексерілген)	4,4	1	Сайт аралық скриптинг
Соқыр SQL инъекциясы	7,8	6	SQL–инъекция
SQL инъекциясы (тексерілген)	7,8	15	
Microsoft IIS Tilda каталогтарын тізімдеу	2,6	1	Ақпараттың ағуы
Сценарийдің бастапқы кодын ашу	2,6	1	
Әлсіз пароль	7,5	2	
Қолданба қатесі туралы хабар	5,0	10	
Нұсқаны ашу ASP.NET	0,0	1	
Microsoft IIS нұсқасын ашу	0,0	1	
Автотолтыру қосылған пароль түрін енгізу	0,0	4	
Каталогты айналып өту	6,8	1	Айналма жолдары
CSRF қорғаусыз HTML пішіні	8,6	6	Функционалдылықты теріс пайдалану
Clickjacking: x–Frame-Options тақырыбы жоқ	6,8	1	
Кіру бетіндегі парольді шабуылдау	6,8	4	

Сканерлеу нәтижелері бойынша жиналған осалдық туралы барлық мәліметтермен қауіпсіздік мамандары жергілікті желілік белсенділік пен құрылғы конфигурацияларымен қатар осалдықтарды бағалаудың жалпы жүйесі (Common Vulnerability Scoring System, CVSS) ретінде тәуекелдерді басымдыққа ие болуы керек. Тәуекел деңгейі анықталған осалдықтардың қайсысы жүйеге шынымен қауіп төндіретінін анықтайды, нәтижеде осалдықтар тәуекел мөлшеріне сәйкес жойылады. Тәуекелдің мәні эксплуатацияны қолдану ықтималдығына байланысты, сондай-ақ, осалдықтың пайда болу жиілігі жүйеде осалдықтың пайда болу күніне байланысты. Осалдық тәуекелінің жиілігі мен сандық деңгейі қауіпсіздік тәуекелінің сандық моделінің математикалық теңдеулерімен анықталады, ол CVSS базалық бағаларын жоғарылату үшін уақыт пен экологиялық өлшемдерді есептейді, содан кейін тәуекелдің соңғы мәнін шығарады. Тәуекел деңгейін сандық бағалау 0-ден 10-ға дейінгі диапазонда болады, бұл сандық бағалауды ұйымдарға осалдықты басқару процестерін дұрыс бағалауға және басымдық беруге көмектесу үшін сапалы көрініске аударуға болады (4-кесте).

Тәуекел деңгейін сандық өлшеу кезінде, эксплуатацияның деңгейімен қатар, біз ескертулердің жалпы саны, эксплуатациялық элемент, әсер етілген параметр және осалдықтарды сканерлеу кезінде анықталған опциялар сияқты көптеген факторларды ескереміз. Тәуекелдерді бағалау нәтижелеріне сүйене отырып, ұсынылған схеманың келесі кезеңі тәуекел деңгейін төмендететін қарсы шаралардың жаңартуларын анықтау болып табылады.

4-кесте. Сапа тәуекелдерін бағалау шкаласы

Тәуекелдің сандық шамасы	Тәуекел санаты	Сипаттамасы
9,0-ден 10,0-ге дейін	Критикалық	Тәуекел мүлдем қолайсыз; пайда болу ықтималдығын азайту үшін дереу әрекет етуді талап етуі керек.
7,0-ден 8,9-ға дейін	Жоғары	Тәуекел қабылданбайды; қалпына келтіру жоспарын мүмкіндігінше тезірек орындау қажет.
4,0-ден 6,9-ға дейін	Орташа	Тәуекел қысқа мерзім ішінде қолайлы болуы мүмкін; болашақ іс-әрекеттерге және бюджеттік жоспарларға тәуекелді азайту жөніндегі шараларды енгізуді талап етеді.
0,1-ден 3,9-ға дейін	Төмен	Тәуекелдер қолайлы; тәуекелді одан әрі төмендету жөніндегі жоспарлар қауіпсіздіктің басқа жаңартуларымен іске асырылуы тиіс.

ҚазҰУ желісінің қауіпсіздігін арттыру үшін анықталған тәуекелдер бойынша келесі ұсыныстар берілген:

1) SQL енгізу: ҚазҰУ университетінің есептеу ортасы SQL енгізу туралы қауіпсіздік жүйесінің тек 21 ескертуін анықтады және келесі элементтер қозғалды: / Login.asp, /Register.asp, /Search.asp, /showforum.asp және / showthread.asp. SQL енгізу шабуылдары хакердің мүддесі үшін бағдарламаның сипатын өзгертетін SQL сұрауларының нысанын өзгертеді. Prepared Statement көмегімен серверлік қорғаныс SQL инъекцияларынан қорғаудың ең тиімді әдісі болып табылады, өйткені сұрау ниеті өзгермейді.

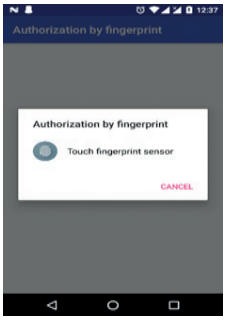
2) Әлсіз пароль: университет желісінде /Login–де әлсіз пароль туралы 6 ескерту табылды. 30 күннен асқан бірнеше пароль шоттары бар, ал кейбіреулері тіпті бір жылға жуық. Парольді бұзу -қазіргі қауіпсіздік деңгейін бағалау үшін қолданылатын ең көп таралған элементтердің бірі. Әлсіз парольдің осалдығын жеңудің қарапайым әдісі - пароль саясатын қолдану, яғни, парольдің ұзындығы 8 таңбадан артық болуы керек, кем дегенде бір бас әріп болуы керек, парольді таңдағанда кем дегенде бір сан және бір арнайы таңба болуы керек.

3) CSRF шабуылдары: осал элементтері /логині бар барлығы 6 нұсқа табылды: asp, /Register.asp және /Іздеу.asp. Негізгі қауіп браузердің сұраныстарды қалай өңдейтініне байланысты. Қарапайым мысал: веб–бағдарлама пароль туралы ақпаратты беру үшін HTTP сұрауында GET әдісін қолданады; get пайдалану кезінде шолғыш форма деректерін URL мекен–жайына кодтайды. Пішін деректері URL мекенжайында болғандықтан, олар шолғыштың мекен-жай жолында көрсетіледі, нәтижеде ақпарат қол жетімді. Ең оңай шешім-POST әдісін қолдану, POST әдісін қолданған кезде форма деректері URL мекенжайында емес, HTTP сұрау хабарламасында көрсетіледі.

Талқылау. Зерттеу көрсеткендей, тәуекелдерді бағалау нәтижелері жоғары басшылыққа, процедуралық, бюджеттік және жүйелік операциялық және басқарушылық өзгерістер туралы шешім қабылдауға көмектесетін ресми есеп форматында құжатталады. Тәуекелдерді бағалау рекурсивті процедура болғандықтан, бұл түпкілікті жасалған есеп тәуекелдерді бағалау процедурасының келесі циклінде ұсынылған құрылымның 1-кезеңі үшін кіріс ретінде пайдаланылады.

ҚазҰУ жүйесінің құпиясөзге байланысты осалдықтарының алдын алу мақсатында мобильді қосымшаға жаңа тексерулер енгізуді ұсынамыз. Ең алдымен, авторизацияланған қолданушы мобильді қосымшаға кірген сәтте саусақ ізі арқылы аутенификация жасалынады, екіншіден авторизацияланбаған қолданушы өз аккаунтына кірген сәтте, мобильді хабарлама аутентификация сұрайды.

11-суретте қосымшаға кіру үшін жасалған жаңа функционал, мұнда мобильді қосымшаға кірген сәтте шығатын аутентификация көрсетілген.

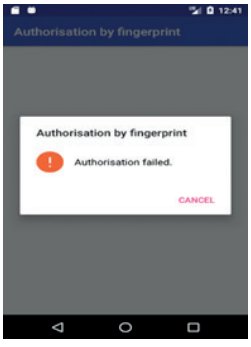


11-сурет. Саусақ ізі бойынша аутентификация

12-суретте қолданушының саусақ іздері, телефонға тіркелген қолданушыны саусақ ізімен сәйкестігі тексеріледі, дұрыс жағдайда біз өзімізге қажетті әрекеттерді жасай аламыз.

12-сурет. Саусақ іздерінің сәйкестігі анықталғаннан кейінгі нәтиже

13-суретте егер қолданушының саусақ іздері телефонда тіркелген саусақ ізіне сәйкес келмеген жағдайда шығатын хабарлама көрсетілген.



13 -сурет. Саусақ іздері сәйкестігі анықталмаған жағдай

14-суретте ҚазҰУ жүйесіне кірген сәтте сұрайтын аутентификация түрі, яғни мобильді қосымшада авторизация жасалған кезде сұралады, ал веб қосымшада міндетті түрде хабарлама сұралады.

14-сурет. Мобильді хабарлама авторизациясы

Қорытынды. Бұл құжат университеттің есептеу ортасы үшін ақпараттық қауіпсіздік тәуекелдерін сандық бағалау құрылымын ұсынады. Ұсынылған модельдің мақсаты қауіпсіздік ережелерін бұзу қаупін азайту болып табылады, бұл кампус желісін осал ететін себептерді түсінуді білдіреді. ҚазҰУ кампус желісіне ұсынылған құрылымды қолдана отырып, желінің қауіпсіздігін қамтамасыз етудің қазіргі тәсілдері университет ортасы тұрғысынан тиімсіз екендігі белгілі болды; өйткені университеттің есептеу ортасы банктер сияқты бұзу мақсаттарынан өзгеше. Бағалау зерттеулері ҚазҰУ желісінде пароль саясатын мәжбүрлеп қолдану сияқты мәселелерді қарастырады. Қашықтан кіруді басқару және рұқсаттарды міндетті есептік жазбалармен шектеу.

Ұсынылған модель университеттің желілік конфигурациясы үшін тәуекел мөлшерін сандық түрде өлшейді және оны нақты және қол жетімді түрде сенімді және қайталанатын тәуекелдерді талдауды жүзеге асыру үшін тәуекел талдаушысы және университеттің қауіпсіздік менеджері қолдана алады. ҚазҰУ зерттелу бойынша авторизация осалдықтары анықталды, сол себепті солардың алын алу шаралары жасалынды, оның ішінде саусақ ізі аутентификациясы және хабарлама авторизациясы. Осы ұсынылған алдын алу шаралары Андроид операциялық жүйесінде қолданба жасалынды, ол REST сұраныс арқылы смартфонмен байланыс жасайды.

Ұсынылған құрылымды кез-келген жоғары білім беру ұйымына

немесе университеттің IT-ортасына қолдануға болады. Бұл университеттерге қауіпсіздікке төнетін қауіп-қатерлерден бір қадам алда тұруға, сонымен қатар, қауіп-қатерге ұшыраған маңызды активтерге назар аудара отырып, қауіпсіздік бюджетінен көбірек алуға мүмкіндік береді.

Information about the authors:

Iztayev Zhalgasbek – Cand. Sci. (Pedagogical), M. Auezov South Kazakhstan University, Shymkent, Kazakhstan, jalgasbek_uko@mail.ru, https://orcid.org/0000-0002-3210-2963;

Dzhusupbekova Gulzat – Cand. Sci. (Pedagogical), M. Auezov South Kazakhstan University, Shymkent, Kazakhstan, gulzat20.10@mail.ru, https://orcid.org/0000-0003-1727-0966;

Ordabayeva Gulzinat – Senior Lecturer, Al-Farabi Kazakh National University; Almaty, Kazakhstan, gulzi200988@mail.ru; https://orcid.org/0000-0001-9952-1620.

ӘДЕБИЕТТЕР:

Ахметов Б.С., Корченко А.Г., Жекамбаева М.Н., Казмирчук С.В. (2015). Қауіптің базалық сипаттамасының кортежді моделі // Қазақстан Республикасының ұлттық ғылым академиясының баяндамалары. – 2015. - №6. – 12-19б. (қазақ тілінде).

Ахметов Б., Қыдыралина Л., Лахно В., Могилный Г., Ахметова Ж., Ташимова А. (2018). Оқу орындарының кибер қауіпсіздігіне өзара инвестициялар бойынша компьютерлік шешімдерді қолдау жүйесінің моделі // Халықаралық машина жасау және технологиялар журналы. – 2018. - Vol.9.-Iss.10.-P.1114-1122 (ағылшын тілінде).

Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. (2017) Жеті қауіпсіз ақпараттық технология/ А.С. Марков ред. басқаруымен.: ДМК Пресс. - 2017. - 224 б.: сурет. (орыс тілінде).

Джаафер Әл-Сарайре, Ала ‘Масарве (2022). Алдыңғы қатарлы қауіп-қатерлерді анықтауға арналған жаңа тәсіл, Мысыр информатика журналы, 2022, ISSN 1110-8665, https://doi.org/10.1016/j.eij.2022.06.005. (https://www.sciencedirect.com/science/article/pii/S1110866522000470, 05.07.2022) (ағылшын тілінде).

И.И. Лившиц (2018). Күрделі өнеркәсіптік объектілерді басқарудың интеграцияланған жүйелерінің ақпараттық қауіпсіздік аудитінің модельдері мен әдістері: техн. ғылымдары докторы дисс.: 05.13.19/ СПИИРАН. - Санкт-Петербург. 2018. -407 б. (орыс тілінде).

Кхайрур Разикин, Бенф ано Соевито (2022). Тәуекелдерді талдау және киберқауіпсіздік құрылымы негізінде ақпараттық қауіпсіздік жүйесін әзірлеу үшін киберқауіпсіздік бойынша шешімдер қабылдауды қолдау моделі, Egyptian Informatics Journal, 2022, ISSN 1110-8665, https://doi.org/10.1016/j.eij.2022.03.001. (https://www.sciencedirect.com/science/article/pii/S1110866522000226, 01.07.2022) (ағылшын тілін-

де).

Кхандо Кхандо, Шанг Гао, Сираджул М. Ислам, Али Салман (2021). Жеке және мемлекеттік ұйымдардағы ақпараттық қауіпсіздік туралы қызметкерлердің хабардарлығын арттыру: Әдебиетке жүйелі шолу, Computers & Security, Volume 106, 2021, 102267, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2021.102267. (https://www.sciencedirect.com/science/article/pii/S0167404821000912, 30.06.2022) (ағылшын тілінде).

Қалимолдаев М.Н., Бияшев Р.Г., О.А. Рог (2017). Ақпаратқа қолжетімділікті шектеу үлгілерін құру үшін логиканы қолдану // Қазақстан Республикасы Ұлттық ғылым академиясының баяндамалары. – Almaty. – 2017.- Vol.3 – Num. 313 (2017). -P.48-54 (орыс тілінде).

ҚР СТ 1698-2007 (2007). Ақпаратты қорғау. Ақпаратты техникалық барлаудан және техникалық есептеу техникасы бойынша жылыстаудан қорғау. Қорғау әдістері. [Электрондық ресурс]// https://online.zakon.kz/Document/?doc_id=30374214&pos=6; -108 #pos = 6; -108. 23.06.2022 (орыс тілінде).

ҚР СТ ГОСТ Р ИСО/МЭК 15408-1-2006 (2006). Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 1-бөлім. Қазақстан Республикасы Индустрия және сауда министрлігінің Техникалық реттеу және метрология комитеті. - 2006. - 100 с. [Электрондық ресурс]// http://db4.sbras.ru/elbib/data/show_page.phtml?22+82. 23.06.2022 (орыс тілінде).

Лахно В., Ахметов Б., Ыдырышбаева М. және Ербол А. (2021). Кибершабуылдарды тану үшін шешімдер қабылдауды қолдау жүйелерінің білім базаларын қалыптастыру модельдері. «Физика-математика ғылымдары». 76. 4 (2021 желтоқсан), 88-98. DOI: https://doi.org/10.51889/2021-4.1728-7901.12. (қазақ тілінде).

Ордабаева Г.К. (2020). Желілік топологияның қауіпсіздік моделі мен әдістерін әзірлеу. Информатика және қолданбалы математика: V Халықаралық ғылыми конференция материалдары (29 қыркүйек -1 қазан 2020 ж.). Алматы, 2020. – б. 367-373 (қазақ тілінде).

Сагар Рахалкар Пуна (2019). Енуді тестілеу бойынша қысқаша нұсқау (NMAP, OpenVAS және Metasploit қолдану арқылы), Махараштра, Үндістан. ISBN-13 (pbk): 978-1-4842-4269-8\ ISBN-13 (electronic): 978-1-4842-4270-4 https: //doi.org/10.1007/978-1-4842-4270-4. https: //www.baikalctf.ru/data/documents/Kratkoe_rukovodstvo_po_testirovaniyu_na_proniknovenie.pdf, 03.07.2022 (орыс тілінде).

Төкеев У.А., Ахметов Б.Б. (2011). Ақпараттық қауіпсіздікті басқару: оқу құралы. – Алматы: әл-Фараби атындағы Қазақ ұлттық университеті, 2011. – 161 б. (қазақ тілінде).

Цифрлық экожүйенің дамытудың 2022-2027 жылдарға арналған («Киберқалқан-2») тұжырымдамасы (2022). [Электронды ресурс] https://www.gov.kz/memleket/entities/mdai/documents/details/320322?lang=kk. 23.06.2022 (қазақ тілінде).

Эрик Филиоль, Франческо Меркальдо, Антонелла Сантоне (2021). Енуге және салдарын жеңілдетуге автоматты тестілеу әдісі: қызыл қалпақ, Procedia Computer Science, том 192, 2021, 2039-2046, ISSN 1877-0509, *https://doi.org/10.1016/j.procs.2021.08.210*. (https://www.sciencedirect.com/science/article/pii/S1877050921017063, 05.07.2022) (ағылшын тілінде).

\

REFERENCES:

Akhmetov B.S., Korchenko A.G., Zhekambaeva M.N., Kazmirchuk S.V. (2015). Motorcade model of basic hazard characteristics//Reports of the National Academy of Sciences of the Republic of Kazakhstan. – 2015. - №6. - gr. 12-19.

Akhmetov B., Kydyralina L., Lakhno V., Mohylnyi G., Akhmetova J., Tashimova A. (2018). Model for a computer decision support system on mutual investment in the cybersecurity of educational institutions // International Journal of Mechanical Engineering and Technology. – 2018. – Vol.9.-Iss.10.-P.1114-1122.

Barabanov A.V., Dorofeev A.V., Markov A.S., Tsirlov V.L. (2017). Seven safe information technologies/edited by A.S. Markova. - M.: DMK Press. - 2017. - 224 S.: silt.

Eric Filiol, Francesco Mercaldo, Antonella Santone (2021). A Method for Automatic Penetration Testing and Mitigation: A Red Hat Approach, Procedia Computer Science, Volume 192, 2021, Pages 2039-2046, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2021.08.210. (https://www.sciencedirect.com/science/article/pii/S1877050921017063, 05.07.2022).

Jaafer Al-Saraireh, Ala' Masarweh (2022). A novel approach for detecting advanced persistent threats, Egyptian Informatics Journal, 2022, ISSN 1110-8665, https://doi.org/10.1016/j.eij.2022.06.005. (https://www.sciencedirect.com/science/article/pii/S1110866522000470, 05.07.2022).

Kalimoldaev M.N., R.G. Biyashev, O.A. Horn (2017). Application of logic for building models of delimitation of access to information//Reports of the National Academy of Sciences of the Republic of Kazakhstan. – Almaty. – 2017.- Vol.3 – Num. 313 (2017).- P.48-54.

Khairur Razikin, Benf ano Soewito (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework, Egyptian Informatics Journal, 2022, ISSN 1110-8665, https://doi.org/10.1016/j.eij.2022.03.001. (https://www.sciencedirect.com/science/article/pii/S1110866522000226, 01.07.2022).

Khando Khando, Shang Gao, Sirajul M. Islam, Ali Salman (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review, Computers & Security, Volume 106, 2021, 102267, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2021.102267. (https://www.sciencedirect.com/science/article/pii/S0167404821000912, 30.06.2022).

Lakhno V., Akhmetov B., Ydyryshbaeva M. and Erbol A. (2021). Models for building knowledge bases of decision support systems for recognizing cyber attacks. «Physical and Mathematical Sciences.» 76, 4 (Dec. 2021), 88-98. DOI:https://doi.org/10.51889/2021-4.1728-7901.12.

Livshits I.I. (2018). Models and methods of auditing information security of integrated systems for managing complex industrial facilities: diss. Doctor of Technology. Sciences: 05.13.19/SPIIRAN. - St. Petersburg. 2018.-407 p.

Ordabaeva G.K. (2020). Development of network topology security model and methods. Informatics and Applied Mathematics: materials of the V International Scientific Conference (September 29 - October 1, 2020). Almaty, 2020. - b. 367-373.

Sagar Rahalkar Pune. (2019). Penetration Test Brief Guide (using NNMAP, OpenVAS and Metasploit), Maharashtra, India. ISBN-13 (pbk): 978-1-4842-4269-8\ ISBN-13 (electronic): 978-1-4842-4270-4 https://doi.org/10.1007/978-1-4842-4270-4. https: //www.baikalctf.ru/data/documents/Kratkoe_rukovodstvo_po_testirovaniyu_na_proniknovenie.pdf, 03.07.2022.

ST RK GOST R ISO/IEC 15408-1-2006 (2006). Information technology. Methods and means of safety assurance. Information Technology Security Assessment Criteria. Part 1. Introduction and general model.//- Committee on Technical Regulation and Metrology of the Ministry of Industry and Trade of the Republic of Kazakhstan. - 2006. - 100 c. [Electronic resource]//http://db4.sbras.ru/elbib/data/show_page.phtml?22+82. 23.06.2022.

ST RK 1698-2007 (2007). Information protection. Protection of information from technical intelligence and from leakage by technical computer equipment. Protection methods. [Electronic resource]// https://online.zakon.kz/Document/?doc_id=30374214&pos=6; -108 # pos = 6; -108. 23.06.2022.

Tokeev U.A., B.B. Akhmetov (2011). Information Security Management: Textbook. - Al-Farabi Kazakh National University, 2011. - Art. 161.

The concept of the development of the digital ecosystem for 2022-2027 (Cyberkalkan-2) (2022). [Electronic Resource] https://www.gov.kz/memleket/entities/mdai/documents/details/320322?lang=kk. 23.06.2022.

МАЗМҰНЫ

СОДЕРЖАНИЕ

CONTENTS

Publication Ethics and Publication Malpracticein
the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethicalguidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any otherlanguage, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:
www:nauka-nanrk.kz
http://physics-mathematics.kz/index.php/en/archive
ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Директор отдела издания научных журналов НАН РК *А. Ботанқызы*
Заместитель директор отдела издания научных журналов НАН РК *Р. Жәлиқызы*
Редакторы: *М.С. Ахметова, Д.С. Аленов*
Верстка на компьютере *Г.Д.Жадыранова*

Подписано в печать 15.09.2022.
Формат 60х881/8. Бумага офсетная. Печать – ризограф.
17,5 п.л. Тираж 300. Заказ 3.

Национальная академия наук РК
050010, Алматы, ул. Шевченко, 28, т. 272-13-19