ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«ҒҰМАРБЕК ДӘУКЕЕВ АТЫНДАҒЫ АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»
коммерциялық емес акционерлік қоғамы
Ақпарттық қауіпсіздік жүйелері кафедрасы

«ҚОРҒАУҒА ЖІБЕРІЛДІ»
Кафедра меңгерушісі т.ғ.қ., доцент Бердібаев Р.Ш.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «_____» _____ 2020 ж.
(қолы)

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: Кәсіпорынның қорғалған веб-сайтын әзірлеу

Мамандығы: 5В100200 – «Ақпараттық қауіпсіздік жүйелері»
Орындаған: Тынышбаев Нурлан Нурболатович Тобы: СИБк-16-1
(аты-жөні)
Ғылыми жетекші: т.ғ.қ., доцент Шайкулова А. А.
(ғылыми дәрежесі, атағы, аты-жөні)
Кеңесшілер:
Мамандығы бойынша:
аға оқытушы Дмитриева Маргарита Валерьевна
(ғылыми дәрежесі, атағы, аты-жөні)
_____«_____»_____ 2020 ж.
(қолы)
Тіршілік қауіпсіздігі бөлімі бойынша:
доцент Жандаулетова Фарида Рустембековна
(ғылыми дәрежесі, атағы, аты-жөні)
_____«_____»_____ 2020 ж.
(қолы)
Мөлшер бақылаушы:
аға оқытушы Альмуратова Камшат Бимуратовна
(ғылыми дәрежесі, атағы, аты-жөні)
_____«_____»_____ 2020 ж.
(қолы)
Пікір беруші:
Төлеулиев Сырым Бимуратович
(ғылыми дәрежесі, атағы, аты-жөні)
_____«_____»_____ 2020 ж.
(қолы)

Алматы 2020

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«ҒҰМАРБЕК ДӘУКЕЕВ АТЫНДАҒЫ АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»
коммерциялық емес акционерлік қоғамы

Басқару және ақпараттық технологиялар институты
Ақпараттық қауіпсіздік жүйелері кафедрасы
5В100200 – «Ақпараттық қауіпсіздік жүйелері» мамандығы

Дипломдық жобаны орындауға берілген
ТАПСЫРМА

Студент: Тынышбаев Нурлан Нурболатович
(аты-жөні)

Жобаның тақырыбы: Кәсіпорынның қорғалған веб-сайтын әзірлеу

2019 ж. «11» қараша №56 университет бұйрығымен бекітілді.

Аяқталған жұмысты тапсыру мерзімі: «____»_____20___ ж.

Жобаға алғашқы деректер (талап етілетін зерттеу (жоба) нәтижелерінің параметрлері және зерттеу нысанының алғашқы деректері):
«Kemel-NT» мектеп оқушыларына арналған веб-сайтты алғашында WordPress платформасында әзірленіп, содан соң веб-сайтқа екі факторлы аутентификация, спам және спам-боттарға қарсы плагиндер орнатылды. Орнатылған қорғаныс әдістері іс жүзінде тексеріліп, сәтті аяқталды. Сонымен қоса дерекқорлар базасына келіп түсетін пайдаланушылардың парольдары MD5 128-биттік хэштеу алгоритмі арқылы шифрланды.

Диплом жобасындағы әзірленуі тиіс мәселелер тізімі немесе диплом жобасының қысқаша мазмұны:
1. Веб-сайттың қазіргі замандағы рөлі
2. Қазақстандағы ақпараттық қауіпсіздік
3. Веб-сайтты қорғау әдістері
4. Қос факторлы аутентификация және т. б. қорғаныс ұйымдастырылған веб-сайт әзірлеу
5. Жұмыс жағдайында табиғи жарықтандыруды, өрт қауіпсіздігін және хабарлағаш санын есептеу.
6. Ақпараттық қауіпсіздік тәуекелдерін екі параметр бойынша бағалау.

Графикалық материалдардың (міндетті түрде дайындалатын сызбаларды көрсету) тізімі:

1.1 кесте – Әзірлеу әдісіне қарай артықшылықтары мен кемшіліктері

1.5 сурет – WordPress платформасындағы reCAPTCHA

2.5 сурет – Веб-сайтты әзірлеу барысында қолданылған плагиндер

2.10 сурет – «Kemel-NT» веб-сайтының дерекқорлар базасы

3.6 сурет – WordPress-тің кірістірілген редакторы

3.14 сурет – Қос факторлы аутентификация сұраудың көрінісі

4.4 кесте – Тәуекелдерді бағалаудың қорытынды кестесі

5.1 кесте – Қауіптер мен зиянды факторлар

5.2 сурет – Шамдарды орналастыру жоспары

Негізгі ұсынылатын әдебиеттер:

1. Т. Хассей WordPress. Создание сайтов для начинающих (+ CD-ROM) / Т. Хассей. - М.: Эксмо, 2016. - 538 с.

2. Гаспарян А. А. Использование CMS при создании образовательных ресурсов // Учен. зап. : науч. журн. / Курск. гос. ун-т. – 2011. – № 3 (19).

3. Абикенова А.А., Санатова Т.С. Безопасность жизнедеятельности. Методические указания к выполнению раздела «Пожарная профилактика» в выпускных работах для всех специальностей. Бакалавриат - Алматы: АИЭС, 2009. - 32 с.

Жоба бойынша жобаның бөлімдеріне қатысты белгіленген кеңесшілер

Бөлімдері	Кеңесшілері	Мерзімі	Қолы
Негізгі бөлім	Шайкулова А. А.		
Өміртішілік			
қауіпсіздігі	Жандаулетова Ф.Р.		
Тәуекелдерді есептеу			
бөлімі	Дмитриева М.В.		

Диплом жобасын дайындау
КЕСТЕСІ

Бөлімдердің атауы, әзірленетін мәселелердің тізімі	Ғылыми жетекшіге ұсыну мерзімдері	Ескерту
Кіріспе	12.02.20 – 15.02.20	орындалды
1.1 Веб-сайттың қазіргу замандағы рөлі	17.02.20 – 10.03.20	орындалды
1.2 Қазақстандағы интернет (Қазнет)	18.02.20 – 05.03.20	орындалды
2 Веб-сайтты әзірлеуге қолданылған технологиялар мен құрал-жабдықтар	13.03.20 – 25.03.20	орындалды
3 Бөлім. Практикалық бөлім	27.03.20 – 16.04.20	орындалды
4 Ақпараттық қауіпсіздіктің тәуекелдерін есептеу	19.04.20 – 15.05.20	орындалды
4.1 Ақпараттық қауіпсіздік		
тәуекелдері	19.04.20 – 02.05.20	орындалды
4.2 Екі параметр бойынша есептеу	02.05.20 – 15.05.20	орындалды
5 Өміртіршілік қауіпсіздігі	08.05.20 – 28.05.20	орындалды
5.1 Жұмыс жағдайын талдау	08.05.20 – 15.05.20	орындалды
5.2 Жасанды жарықтандыруды есептеу	15.05.20 – 28.05.20	орындалды

Тапсырманың берілген уақыты «12 » қаңтар 2020 ж.

Кафедра меңгерушісі _____ (Бердібаев Р.Ш.)
(қолы) (аты-жөні)

Жобаның
ғылыми жетекшісі _____ (Шайкулова А. А.)

(қолы) (аты-жөні)

Орындалатын тапсырманы
қабылдаған студент _____ (Тынышбаев Н. Н.)
(қолы) (аты

Аңдатпа

Дипломдық жоба «Kemel-NT» білім беру орталығының қорғалған веб-сайтын әзрлеуге арналған.

Веб-сайттың қазіргі замандағы рөлі, танымалдылығы, оған төнетін қауіптер мен оларды қорғаудың маңыздылығы мен тәсілдері талданған.

Веб-сайтты әзірлеуде WordPress сайт әзірлеу платформасы, дерекқор ұйымдастыру үшін phpMyAdmin технологиясы қолданылды.

Қорғау технологиясын ұйымдастыру үшін қос факторлы аутентификация, спам-боттардан қорғауға арналған Aksimet программасы, парольдік қорғау механизмі МД5 қолданылды. Дипломдық жобада қауіпсіздік механизмдерін қамтамасыз етуде аутентификация, тұпнұсқалықты анықтау, авторландыру және парольдік қорғаудың сенімді механизмдері жүзеге асырылған.

Аннотация

Дипломный проект предназначен для разработки защищенного веб-сайта образовательного центра «Kemel-NT».

Проанализирована современная роль веб-сайта, популярность, угрозы и значение и способы их защиты.

При разработке веб-сайта использовалась платформа WordPress, а также используется технология phpMyAdmin для организации базы данных.

Для организации технологии защиты использовалась двойная аутентификация, программа Aksimet для защиты от спамов и спам-ботов, механизм парольной защиты MD5. Дипломный проект реализует надежные механизмы идентификации, аутентификации, авторизации и защиты паролем для обеспечения механизмов безопасности.

Annotation

The graduation project is intended to develop a secure website for the «Kemel-NT» Educational Center.

The modern role of the website, popularity, threats and significance and ways to protect them are analyzed.

When developing the website, the WordPress platform was used, and phpMyAdmin technology was used to organize the database.

For the organization of protection technology, double authentication was used, Aksimet program for protection against spam and spam bots, the password protection mechanism MD5. The graduation project implements reliable mechanisms for identification, authentication, authorization and password protection to ensure security mechanisms.

Мазмұны

Кіріспе

XXI ғасыр – бұл ақпараттық технологиялардың ғасыры. Жаңа ақпараттық-коммуникациялық технологияларды кеңінен қолдану әлем дамуындағы қайтымсыз процесс және соңғы онжылдықтағы ғылыми-технологиялық революция болып табылады. Қазіргі таңда адамдар әр түрлі себептермен Ғаламтор (World Wide Web) сияқты ақпарат көзіне жүгінеді.

Мамандардың айтуынша, көп ұзамай барлық отбасылар Ғаламторды күн сайын қолданады. Бұл кез-келген ақпараттық технологияның иесі оны қызықтыратын кез-келген мақалалар, суреттер, бейне немесе аудио ақпараттарды жүктей алатын уақыт болады. Ол бұл ақпаратты қалаған кезде ала алады. Біраз уақыттан кейін жасанды интеллект жүйелері - параллель машиналық аударма, сондай-ақ дауысты сәйкестендіру және тану соңғы ұлттық және тілдік кедергілерді жойып, ақысыз ақпарат алмасуға мүмкіндік береді.

Ақпараттық технологиялар өркениет прогресінің жетекші факторларының бірі болды, ал оларды жаппай пайдалану қоғамдық қатынастардың жаңа саласын қалыптастырды. Ақпараттық технологиялар әлеуметтік және экономикалық дамудың, мемлекеттік басқарудың, адамдардың күнделікті өмірінің әр түрлі тараптарына әсер етеді. Олар телекоммуникациялық технологиялармен қатар ақпараттандыру, ақпараттық қоғамға қозғалыс процестерінің негізін құрайды. Қазақстан Республикасында ақпараттық технологияларды дамыту және тиімді пайдалану мемлекеттік саясаттың басым бағыттарының бірі болып табылады.

Бүгінгі күні әрбір ұйымның жеке web-сайттары бар. Қазіргі заманғы ақпараттық технологияларды пайдалану жағдайында – бұл жарнамалық қызмет өрісін кеңейтуге және сол арқылы қосымша клиенттерді тартуға мүмкіндік беретін Өмір сүрудің қажетті факторы.

Сайттарды жасау және әзірлеу:

- сайтты әзірлеуге бастапқы техникалық тапсырманы бекіту;
- сайттың құрылымдық сұлбасын анықтау - бөлімдердің, контенттің және навигацияның орналасуы;
- веб-дизайн-сайт макетінің графикалық элементтерін, шарлау мәнерлері мен элементтерін жасау;
- жобада қажетті бағдарламалық кодты, модульдерді, деректер базасын және сайттың басқа да элементтерін әзірлеу;
- интернет желісінде сайтты тестілеу және орналастырудан тұрады.

Мұндай ақпараттық технологиялардың дамуының кері әсері, ол әрине қолданушылардың жеке деректеріне қауіп төнетін қауіптер. Қауіпсіздік қатерлері бірнеше факторлармен байланысты: бірінші кезекте бұл веб-қосымшалардың немесе олардың компоненттерінің осалдығы. Екіншісі – сәйкестендіруді тексеру механизмдерінің осалдығы. Үшінші кезекте қауіпсіздік қатерлері қолданушылардың өздерінің шабуылдарына, клиент-сайд шабуылдарына байланысты. Қауіптердің төртінші түрі – сыни

ақпараттың шығуы немесе жария етілуі. Қауіптің бесінші түрі – логикалық шабуылдар.

Веб-қосымшалардың ақпараттық қауіпсіздік қауіптерінің негізгі түрлері:

- Құпиялылық қаупі-деректерге рұқсатсыз қол жеткізу.
- Тұтастық қаупі-деректерді рұқсатсыз бұрмалау немесе жою.
- Қол жетімділік қатерлері-деректерге қол жетімділікті шектеу немесе бұғаттау.

Веб-қосымшаның ақпараттық қауіпсіздік қатерінің негізгі көзі сыртқы бұзушылар болып табылады. Сыртқы бұзушы-әдетте, коммерциялық қызығушылықпен дәлелді, компанияның сайтына кіру мүмкіндігі бар, зерттелетін ақпараттық жүйе туралы білімі жоқ, желілік қауіпсіздікті қамтамасыз ету мәселелерінде жоғары біліктілігі және ақпараттық жүйелердің түрлі түрлеріне желілік шабуылдарды іске асыруда үлкен тәжірибесі бар тұлға.

Бұл дипломдық жобаның мақсаты – адаптивті интерфейсі бар қорғалған веб-сайтты әзірлеу.

Осы мақсатты жүзеге асыру келесі міндеттерді мазмұнды және әдістемелік шешуді талап етеді:

- Қазақстандағы ақпараттық қауіпсіздікпен танысу және зерттеу;
- WordPress платформасында сайтты әзірлеу;
- Web-сайтты қорғаудың жолдары мен мүмкіндіктері;
- әзірленген технологияны нақты сынақтан өткізу.

1 Бөлім (Аналитикалық бөлім)

1.1 Web-сайттың қазіргі замандағы рөлі

Бұл тақырыптың өзектілігін талқыламай тұрып, бірінші веб-сайттың не екенін біліп алайық.

Веб-сайт – бірдей домендік атауды пайдаланатын, жалпыға қол жетімді, өзара байланысты веб-беттердің жинағы. Веб-сайттарды әртүрлі мақсаттар үшін жеке адам, кәсіпорындар, бизнес немесе ұйым қолдана алады. Жалпыға қол жетімді барлық веб-сайттар бүкіләлемдік ғаламторды құрайды.

Веб-сайттар шексіз әртүрлілікке ие, соның ішінде білім беру сайттары, жаңалықтар сайттары, форумдар, әлеуметтік медиа сайттары, электрондық коммерция сайттары және басқалар. Сайт парақтары әдетте мәтін мен басқа ақпарат құралдарының қоспасы болып табылады. Алайда, веб-сайттың нысанын белгілейтін ережелер жоқ. Адам веб-сайтты раушанның ақ-қара суреттерінен немесе «мысық» сөзінен басқа ештеңе жазбай жасай алады. Дегенмен, көптеген сайттар, сайттағы басқа санаттар мен мазмұндарға сілтеме жасайтын негізгі беттің шаблоны бойынша жүреді. Алдымен веб-сайттар жоғары деңгейлі домен бойынша жіктелді. Мысалға: мемлекеттік веб-сайттар = .gov, оқу орнының веб-сайттары = .edu, коммерциялық емес веб-сайттар =.org, коммерциялық веб-сайттар = .com және де ақпараттық сайттары = .info домендерімен негізделген болатын. Бұл жоғарғы деңгейлі домен кеңейтімдері әлі де бар. Қазіргі заманғы интернетте әр елдің өзінің кеңейтімдері бар, дегенменде домендер арасында ең танымалы ол – .com кеңейтімі болып есептеледі.

Веб-сайттар әзірлеу әдісіне қарай екі түрге жіктеледі:

- Статикалық веб-сайт. Бұл мазмұнды алу үшін деректер базасына кіре алмайтын сайттар. Әдетте, сайт иесі әр бетте қамтылған ақпаратқа үнемі өзгертулер енгізуді қажет етпейтін жағдайда, тұрақты веб-сайт қолданылады;
- Динамикалық веб-сайт. Бұл мазмұнды алу үшін деректер базасына жүгінетін және веб-сайт беттерінде деректер базасынан алынған нәтижелерді көрсететін адамдар.

1.1 кесте – Әзірлеу әдісіне қарай артықшылықтары мен кемшіліктері

Статикалық веб-сайт	Динамикалық веб-сайт
Артықшылықтары: статикалық сайттар пайдалануда арзан. HTML-құжаттар бір рет жасалады және еш өзгеріссіз жеткізіледі. Егер де мерзімді ақпаратты ұсыну үшін статикалық веб-сайт пайдаланылса, ол динамикалық веб-сайтқа қарағанда аз техникалық қызмет көрсетуді талап етеді. Олар сондай-ақ әлдеқайда жылдам, өйткені веб-	Артықшылықтары: динамикалық веб-сайттар өзінің икемділігімен жеңеді. Веб-мазмұн мен макеттің қатаң бөлінуінен, мазмұнның өзгеруін пайдаланушылар бағдарламалаудың қандай да бір бұрынғы білімдерінсіз ақ жасай алады. Әдетте мәтіндік редактор көмегімен. Динамикалық веб-сайттар, сондай-ақ, олар пайдаланушы енгізген деректерге

сайттар серверге ешқандай өзгерістерсіз жүктеледі.	жауап бере алатын артықшылығы бар.
Кемшіліктері: ескірген ақпаратты статикалық сайттың HTML-беттерінде қолмен ауыстыруға тура келеді, бұл бағдарламалау саласында тиісті білімді талап етеді. Сонымен қатар, HTML-құжаттарды веб-серверге жіберу үшін де FTP-бағдарламау тілін білу қажет.	Кемшіліктері: динамикалық веб-сайтты құру үшін әдетте басқару жүйесін білу қажет (CMS немесе интернет-дүкендер жүйесі). Жүйені конфигурациялау үшін негізгі HTML білімінен басқа Perl немесе PHP сияқты қосымша бағдарламалау тілі қажет. Жүйе орналасқан серверде мәліметтер базасы болуы керек. Жобаның көлеміне байланысты динамикалық веб-сайттар тұрақты веб-жобаларға қарағанда әлдеқайда көп серверлік ресурстарды қажет етеді.

Функционалды мақсатына қарай сайттар былай жіктеледі:

Сайт-визитка. Сайттардың ең қарапайым түрі. Іс жүзінде әдеттегі қағаз визиткасының электрондық нұсқасы. Сайт-визиткада компания, оның байланыстары және негізгі көрсетілетін қызметтер туралы негізгі ақпарат болады. Әдетте мұндай сайт CMS көмегімен статикалық немесе динамикалық болуы мүмкін және бір немесе екі беттен тұрады;

Корпоративті веб-сайт. Мұндай веб-сайттар визиткалардан динамикалық мазмұнның болуымен ерекшеленеді. Атап айтқанда, бұл компания мен оның серіктестері туралы жаңалықтар, ұсынылатын тауарлар мен қызметтердің жаңартулары, арнайы ұсыныстар, компания өміріндегі оқиғалар, сондай-ақ фотогалерея болуы мүмкін. Мазмұнның жеткілікті мөлшерде болуы іздеу жүйесін веб-сайтқа енгізуді қамтиды. Корпоративтік веб-сайт клиенттер мен компания арасындағы қарым-қатынастың онлайн механизмдерін ұсына алады, мысалы, бұл онлайн-кеңесшінің немесе сайттан қоңырау шалу модульдері болуы мүмкін.

Ақпараттық портал. Атауынан көрініп тұрғандай, мұндай веб-сайт әдетте кез-келген сала, өнім санаты немесе қызмет көрсету саласы туралы нақты ақпараттың үлкен көлемін (техникалық сипаттамалар, құжаттар, презентациялар, мамандарға нұсқаулар және т.б.) қамтиды.

Веб-сайттың функционалдығы мақалаларды (блогты) жариялау тетігін және олардың санатын, ыңғайлы іздеу тетіктерін және сайт картасын қосады. Әдетте пайдаланушыларға Интернетте ұсынылған ақпаратты талқылауға, сапасы мен маңыздылығын бағалауға мүмкіндік беріледі. Пайдаланушыларды тіркеуге және авторизациялауға, хабар алмасуға жағдай жасайды;

Интернет-дүкен. Интернет-дүкендер көбінесе іс-жүзінде жүзеге асыру үшін ең қиын және қымбат болып табылады, өйткені олар жоғарыда аталған барлық веб-сайттардың функционалдығын қамтиды және сонымен бірге

тауарлар мен қызметтерді сатудың және онлайн сатудың түрлі тетіктерін ұсынады.

Интернет-дүкеннің веб-сайты әдетте компанияның негізгі сатылым құралы болып табылады, сондықтан оны дамыту және қолдау қажетті сапа мен функционалдылыққа қол жеткізу үшін қомақты ақшалай қаражат талап етеді.

Шағын және орта компаниялар интернет-дүкенді жүзеге асыратын платформа ретінде CMS мамандандырылған түрлерін пайдаланады. Ірі интернет-дүкендердің веб-сайттарын нөлден сатады, өйткені клиенттердің көпшілігінде CMS өнімділігі жеткіліксіз болуы мүмкін. Сонымен қатар, ірі интернет-дүкендер әртүрлі қызметтердің, тетіктердің, деректер көздерінің және т.б. интеграциялық жүйені ұсынады, оны тек өздігінен жазылған шешімді қолдана отырып жүзеге асыруға болады.

Қазіргі заманда сайтты құрудың өзектілігі, егер сіз ақпаратты көптеген адамдарға мүмкіндігінше тез жеткізгіңіз келсе, оны сіз веб-сайттың көмегімен іске асыра аласыз. Веб-ресурс сізге компания туралы және оның өнімдері немесе қызметтері туралы ақпаратты дәл және бір уақытта толық көлемде ұсынуға мүмкіндік береді. Сондай-ақ, сайт компания жаңалықтары туралы, бағаның өзгеруі немесе жұмыс режимі туралы, ризашылық білдіретін клиенттердің пікірлері туралы есеп бере алады.

Әрбір компанияға күрделі дизайн және функционалдығы бар үлкен портал қажет емес. Кейде шағын бизнес картасының сайты жеткілікті, оны өзіңіз жасай аласыз немесе оны кәсіпқойларға аз ақыға тапсырыс бере аласыз.

Веб-сайтты әзірлеудің өзектілігі келесі факторлармен түсіндіріледі:

- Ақпараттың кең ауқымды адамдарға берілу жылдамдығы;
- Компанияның имиджін жақсарту және оның танымалдылығын арттыру;
- Клиенттердің кері байланысын ұйымдастыру мүмкіндігі;
- Еліміздің әр түкпірінде және шетелде филиалдармен және өкілдермен жедел байланыс;
- Маркетингтік зерттеулерді ұйымдастыру;
- Жарнама және сатып алушылар мен клиенттерді тарту;
- Трафиктің көбеюі.

2020 жылдың басында 4,5 миллиардтан астам адам интернетті пайдаланады, ал әлеуметтік желілер аудиториясы 3,8 миллиардтан асып кетті. Әлемдік халықтың 60% - ға жуығы онлайн режимінде, және 100 жылдық орта шегінде әлемдегі барлық адамдардың жартысы әлеуметтік желілерді пайдаланатын болады деп болжауға барлық негіздер бар.

«We Are Social» және «Hootsuite» компаниясының «Digital 2020» ғаламдық есеп статистикасы бойынша сандық технологиялардың мәні жаңа биіктерге жетті, және көптеген адамдар интернетте көп уақыт өткізіп, онда көп міндеттерін шешуде:

- Әлемдегі Интернет пайдаланушыларының саны 4,54 миллиард адамға жетті, бұл өткен жылмен салыстырғанда 7% -ға көп (2019 жылдың қаңтарымен салыстырғанда +298 млн. Жаңа пайдаланушылар).
- 2020 жылдың қаңтарында әлемде 3,80 миллиард әлеуметтік желіні пайдаланушылар болды, әлеуметтік медиа аудиториясы 2019 жылмен салыстырғанда 9% өсті (бұл жылына 321 миллион жаңа қолданушы).
- Бүгінгі таңда ұялы телефондарды 5,19 миллиардтан астам адам пайдаланады - бұл өткен жылмен салыстырғанда 124 миллионға (2,4%) көп.

Орташа пайдаланушы күн сайын Интернетке 6 сағат 43 минутын жұмсайды. Бұл бір жыл бұрынғы статистикаға қарағанда 3 минутқа аз, бірақ әлі күнге бір пайдаланушыға 100 күннен асады. Егер сіз күніне шамамен 8 сағат ұйқыға кететіретін болсаңыз, ал қалған уақыттың 40%-дан астамын Интернетте өткземіз дегенді білдіреді.

Әлемдік ғаламтор аудиториясы бір уақытта 2020 жылы 1,25 миллиард жыл желіде болады, ал уақыттың үштен бірі әлеуметтік желілерге шығады. Адамдардың Интернетте өткізетін уақыты әр елдерде әр қалай. Сонымен ең ұзақ уақыт, ол – Филиппинде, олар күніне 9 сағат 45 минут жұмсаса, ал ең қысқасы Жапонияда - 4 сағат 22 минут жұмсайды.

Әрине, мұндай статистика ақпараттық технологиялардың тоқтаусыз дамып жатқанын көрсетеді. Осыншама үлкен ақпараттар сақталатын әлеуметтік желіге төнетін қауіптерде аз емес екені айқын.

1.2 Қазақстандағы интернет (Қазнет)

Қазнет – интернет желісіне қол жеткізуді қамтамасыз ететін ақпараттық технологиялар мен инфрақұрылым жиынтығы, сондай-ақ жоғарғы деңгейдегі қазақстандық домендік атауларды пайдаланатын Қазақстан аумағындағы электрондық ресурстардың хостингі.

Қазақстандағы интернет Дүниежүзілік Желінің құрамдас бөлігі ретінде Қазақстанның Республикасының байланыс және ақпарат министрлігінің құзыретіне жатады. Қазнеттің дамуына алғаш жол ашқан Ұлттық провайдер — "Қазақтелеком" және "Транстелеком" үлкен рөл атқарады.

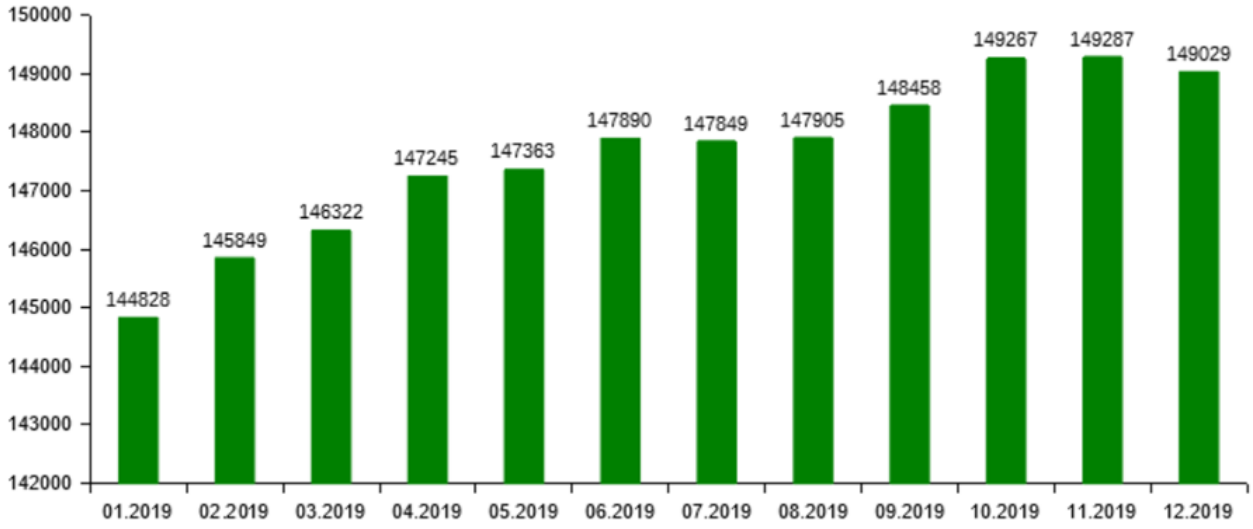
Қазақстан Республикасының заңнамасына сәйкес 2001 жылдың 3 мамырында қабылданған "Бұқаралық ақпарат құралдары туралы" ҚР 1999 жылғы 23 шілдедегі № 451-1 Заңына, сондай-ақ 2009 жылғы 10 шілдедегі "Қазақстан Республикасының кейбір заңнамалық актілеріне ақпараттық-коммуникациялық желілер мәселелері бойынша өзгерістер мен толықтырулар енгізу туралы" Қазақстан Республикасының заңына түзетулер негізінде барлық сайттар БАҚ мәртебесіне ие болды. Осының негізінде барлық интернет-ресурстар: веб-сайттар, чаттар, блогтар, интернет-дүкендер, электрондық кітапханалар және т.б. — тиісті қылмыстық, азаматтық және әкімшілік жауапкершілігі бар бұқаралық ақпарат құралдарына теңестіріледі. Қазақстан заңнамасын бұзатын кез келген ресурстар серверді орналастыру және доменді тіркеу еліне қарамастан, ел ішінде қол жеткізуден ажыратылуы мүмкін.

2009 жылдан бастап Қазақстан Республикасының ААЖ аясында (қазіргі - Қазақстан Республикасы Ақпарат және коммуникациялар министрлігі) компьютерлік инциденттерге әрекет ету қызметі құрылады (шетелдік CERT ұйымының қызметтеріне ұқсас). Жаңа бөлімнің міндеті компьютерлік және ақпараттық технологияларды пайдалану саласындағы құқық бұзушылықтардың алдын алу бойынша мемлекеттік органдардың, байланыс операторларының, сондай-ақ ұлттық ақпараттық инфрақұрылымның басқа да субъектілерінің компьютерлік қауіпсіздігін үйлестіру болып табылады. Сонымен қатар, оның міндетіне ақпараттық қауіпсіздіктің қазіргі қауіптері мен қолданылатын қорғау құралдарының тиімділігі туралы ақпарат жинау, талдау және жинақтау кіреді.

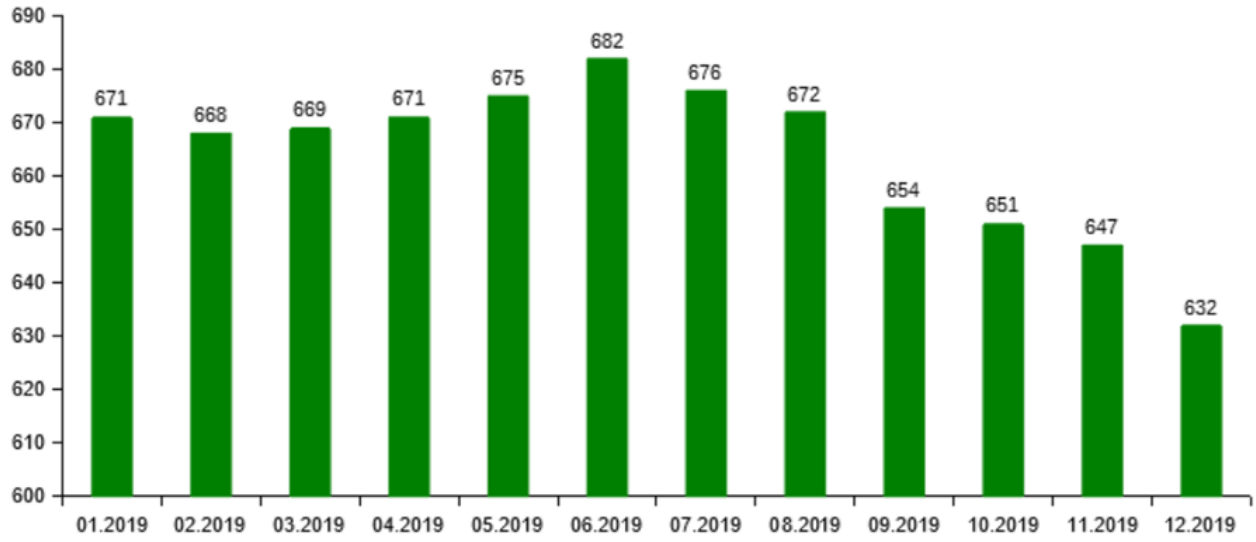
Қазақстандық Интернет сегментінің кеңістігіндегі доменіне әкімші - бұл «Қазақстандық IT-компаниялар қауымдастығы» болып қабылданды, ал домендік атауларды тіркеуші - «Қазақ желілік ақпарат орталығы» мекемесі (KazNIC) тағайындалды.

«Digital 2020» бағдарламасы аясында Қазақтстанның осы жылдың басындағы статистаклық көрсеткіші:

- Қазақстандағы Интернет пайдаланушыларының саны 14,73 миллион адамға жетті, бұл өткен жылмен салыстырғанда 4,5% -ға көп (2019 жылдың қаңтарымен салыстырғанда +637 мың жаңа пайдаланушы).
- Әлеуметтік желіні пайдаланушылардың саны 9,5 миллион адамға жеткен, яғни Қазақстандақтардың 51%-ын қамтиды. Бұл көрсеткіш 2019 жылмен салыстырғанда 26%-ға артқан (+1,9 миллион).
- Қазақстандағы интернеттің орташа жылдамдығы 19,59 мг/с.



1.1 сурет – Қазақстандағы .kz домендік атауының өсу динамикасы



1.2 сурет – Қазақстандағы .қаз домендік атауының өсу динамикасы

Веб-сайттардың 2019 жылғы көрсеткіші бойынша:

- SSL-сертификатын пайдаланатын веб-ресурстардың саны 50%-ға өсті. Қазір Қазнеттегі сертификатты пайдаланушылар саны 18 000-ға жуық;
- Қазнеттегі 150 мыңға жуық сайттың тек 89 мыңы ғана қол жетімді, ал қалғандары түрлі себептермен қолдансытан шыққан (хостинг мерзімінің бітуі және т.б себептер);
- CMS Wordpress әлі де Қазақстанда көшбасшы. Joomla өткен жылмен салыстырғанда рейтингі екі есеге төмен түскен;
- NGINX – 86%-дық нарық үлесі бар ең танымал веб-сервер болып табылады.

1.3 Қазақстандағы ақпараттық қауіпсіздік

Ақпараттық және компьютерлік технологиялардың дамуымен ақпараттық және киберқауіпсіздікке қатысты мәселелерді құқықтық реттеу мәселелері күннен-күнге танымал болып, өзектілігі артуда.

Қауіпсіз IT-инфрақұрылымның негізі:

- Тұтастық – бұл ақпарат өзгеріссіз, дұрыс және шынайы болып қалуының кепілі. Пошта хабарламасы қайта жіберілген кезде өзгертілмеуін қамтамасыз ететін шаралар мысал бола алады;
- Қол жетімділік – бұл рұқсат етілген пайдаланушыларға қажетті активтерді, ресурстарды және жүйелерді қажетті өнімді қамтамасыз ете отырып, қол жеткізуге және олармен жұмыс істеуге мүмкіндік береді. Бұған мысал қол жеткізуді қорғау және пошта қызметіне өткізу қабілеттілігін беру;
- Құпиялылық – бұл ақпаратты оқуға және түсіндіру мүмкіндігіне кепілдік берілген адамдар және процестер. Мысал ретінде адресаттан басқа ешкім оқымауынан қорғалған пошта хабарламасы болады.

Ақпарат басқа маңызды іскерлік активтерге ұқсас ұйым бизнесі үшін үлкен маңызға ие және тиісінше қорғалуы тиіс актив болып табылады. Ақпараттық қауіпсіздік – ақпаратты иеленушілерге немесе пайдаланушыларға залал келтірумен, сондай-ақ ақпараттық саладағы адамның және азаматтың, қоғам мен мемлекеттің құқықтары мен

мүдделерінің шынайы және ықтимал қауіптерден ақпараттың және қолдаушы инфрақұрылымның қорғалуы, онда тұрақты даму мен ақпараттық тәуелсіздік қамтамасыз етіледі. Ақпараттық қауіпсіздікті қамтамасыз ету немесе ақпаратты қорғау деп оның құпиялылығын, тұтастығын және қол жетімділігін сақтау болып табылады. Ақпараттық қауіпсіздік саясатқа, рәсімдерге, процестерге, ұйымдық құрылымдарға және бағдарламалық-техникалық құралдардың функцияларын қоса алғанда, бақылау шараларының тиісті жиынтығын іске асыру арқылы қол жеткізіледі.

Ақпараттық қауіпсіздік саясаты – ақпаратты, оның ішінде таратылуы шектеулі ақпаратты (қызметтік ақпарат), ақпараттық процестерді қорғау жөніндегі алдын алу шараларының кешені және өз қызметінде Қазақстан Республикасы Энергетика министрлігінің, оның үкімдері мен үкіметке бағынысты ұйымдарының ақпараттық жүйелерін пайдаланушылардың атына қойылатын талаптарды қамтиды. Қазақстан Республикасының ақпараттық қауіпсіздік саясаты – "Ақпараттандыру туралы" 2015 жылғы 24 қарашадағы № 418-V Қазақстан Республикасының Заңы және "Қазақстан Республикасында ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі кейбір шаралар туралы" Қазақстан Республикасы Үкіметінің 2004 жылғы 14 қыркүйектегі № 965 қаулысы негізінде Министрліктің орталық аппаратында ақпаратты қорғау жүйесін тікелей ұйымдастыру (құру) және тиімді жұмыс істеуін қамтамасыз ету үшін ақпараттық технологиялар және мемлекеттік қызметтер Департаменті құрылды.

Ақпараттық қауіпсіздік шешімдерін жүзеге асыру аясында жұмыс тобы құрылып, келесі міндеттемелер қойылды: ақпараттық қауіпсіздік саласындағы жағдайды талдау, болжау және ақпараттық қауіпсіздік тәуекелдерін анықтау. Осы Саясаттың талаптары Министрліктің барлық құрылымдық бөлімшелеріне, инфрақұрылымына, Министрліктің ұйымдарына қолданылады және барлық қызметкерлер мен лауазымды адамдар үшін міндетті болып табылады. Саясаттың негізгі ережелері Министрлікпен, оның үкіметке бағыныстағы ұйымдармен ақпаратты, қызметтерді жеткізушілер және тұтынушылар ретінде өзара іс-қимыл жасайтын және ішкі нормативтік, әдістемелік құжаттар мен келісімдерде қолдануға болатын басқа ұйымдарға, мекемелерге қолданылады.

Министрлікте, оған бағынышты ұйымдардың ақпараттық қауіпсіздікті қамтамасыз етудегі негізгі принциптері:

- Қазақстан Республикасы заңнамасының талаптарын сақтау;
- Қазақстан Республикасының аумағында қолданылатын ақпараттық қауіпсіздік саласындағы халықаралық және ұлттық стандарттардың сақталуы;
- ақпараттық активтердегі осалдықтарды анықтау мақсатында ақпараттық кеңістікті үнемі және жан-жақты талдау;
- ықтимал проблемалардың себеп-салдарының байланыстарын анықтау және олардың негізінде нақты даму болжамын құру;

- анықталған проблемалардың Министрліктің, оның үкімдері мен Министрліктің қарамағындағы ұйымдардың мақсаттарына әсер ету дәрежесін бағалау;
- қорғаныс шараларын тиімді орындау;
- ақпараттық қауіпсіздікті қамтамасыз етудің қол жетімділігі мен бағалау мүмкіндігі, қорғаныс шараларын қолдану нәтижесі анық (айқын) болуы керек және тиісті уәкілеттік берілген маманмен бағалану.

Министрліктің, оның үкіметке бағынысты ұйымдарының ақпараттық қауіпсіздігін қамтамасыз етудің негізгі мақсаты:

- қаржылық және материалдық-техникалық құралдарды ұрлау арқылы оның қызметіне зиян келтірудің алдын алу;
- мүлік пен құндылықтарды жою;
- құпия ақпараттар көздерін ашу, тарату және рұқсатсыз кіру;
- ақпараттандыру құралдарын қоса алғанда, өндірістік қызметті қамтамасыз етудің техникалық құралдарының бұзылуы, сонымен қатар қызметкерлерге зиян келтірудің алдын алу.

Қауіпсіздік жүйесінің міндеттері:

- кәсіпорынның, оның құрылымдық бөлімшелері мен қызметкерлерінің құқықтарын қорғау;
- қаржылық, материалдық және ақпараттық ресурстарды сақтау және тиімді пайдалану;
- қызметтердің сапасы мен пайдаланушылардың қауіпсіздігін қамтамасыз ету арқылы кәсіпорынның имиджін жақсарту.

Осыдай заңнамалар мен міндеттемелердің арқасында Қазақстан Жаһандық киберқауіпсіздік индексінде (Global Cybersecurity Index) өз позициясын қарқынды жақсартуда. Соңғы есепте Қазақстан бірден 40-шы орынға көтерілді. Өткен жылдың рейтингісінде еліміз 82-ші орынды иеленді.

Сарапшылар елдің заң саласындағы жетістіктерін атап өтеді. Атап айтқанда, Қазақстан ақпараттық-коммуникациялық технологиялар мен ақпараттық қауіпсіздік саласындағы талаптарды біріздендірді. Цифрландыру жөніндегі бастама киберқауіпсіздіктің тиімді стратегиясына үлкен мән беруде. Соңғы екі жыл ішінде елімізде киберқауіпсіздік саласын дамытудың негізгі тұжырымдамалық тәсілдері жасалды. «Қазақстанның кибер қалқан» киберқауіпсіздік тұжырымдамасы, сонымен қатар бірқатар заңнамалық актілер мен салалық бұйрықтардың көпшілігі әзірленді және бекітілді. Сонымен қатар, зиянды кодты зерттеуге арналған сынақ зертханалары құрылды, ұлттық ақпараттық қауіпсіздікті үйлестіру орталығы іске қосылды, осы мамандық бойынша гранттар саны көбейді.

«Қазақстанның кибер қалқаны» киберқауіпсіздік бағдарламасын белсенді іске асыру 2018 жылы басталып, 2022 жылға дейін жасалған. Қазақстанның тұңғыш Президенті Нұрсұлтан Назарбаев алғаш рет 2017 жылғы қаңтарда жыл сайынғы халыққа арнаған Жолдауында Қазақстанда киберқылмыспен күресу үшін арнайы қорғаныс жүйесін құру қажеттігін мәлімдеді. Содан кейін ол Үкіметке және ҰҚК-не «Қазақстанның кибер қалқаны» жүйесін құру бойынша шаралар қабылдауды тапсырды.

1.2 кесте – Қазақстан Республикасының киберқылмыстың алдын алу үшін қабылданған заңнамалары мен оған тағайындалатын жазалар

205-бап. Ақпаратқа, ақпараттық жүйеге немесе телекоммуникация желісіне заңсыз қол жеткізу	1. Азаматтардың немесе ұйымдардың құқықтары мен заңды мүдделерін немесе қоғамның немесе заңмен қорғалатын мемлекеттің мүдделерін елеулі түрде бұзуға әкеп соқтыратын ақпараттық жүйеде немесе телекоммуникация желісіндегі электрондық бұқаралық ақпарат құралдарында заңмен қорғалатын ақпаратқа қасақана заңсыз қол жеткізу: үш жүз айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға, не сол мөлшерде түзеу жұмыстарына, не екі жүз қырық сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға, не жетпіс бес тәулікке дейінгі мерзімге қамаққа алуға жазаланады. 2. Осы акт мемлекеттік электрондық ақпараттық ресурстарға немесе мемлекеттік органдардың ақпараттық жүйелеріне қатысты жасалынса: белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан екі жылға дейінгі мерзімге айыра отырып немесе бес жүз айлық есептік көрсеткішке дейінгі мөлшерде айыппұл салуға, не сол мөлшерде түзеу жұмыстарына не үш жүз сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға, не тоқсан тәулікке дейінгі мерзімге қамаққа алуға жазаланады.
206-бөлім. Ақпаратты заңсыз жою немесе өзгерту	1. Ақпарат жүйесінде сақталған немесе телекоммуникациялық желілер арқылы берілетін электрондық

	тасымалдағышта сақталатын ақпаратты заңсыз түрде қасақана жою немесе өзгерту, сондай-ақ егер ақпарат азаматтардың немесе ұйымдардың немесе қорғалатын ұйымдардың құқықтары мен заңды мүдделерін елеулі түрде бұзуға әкеп соқтырса, ақпараттық жүйеге көрінеу жалған ақпарат енгізу. қоғам немесе мемлекет мүдделерінің заңы: айлық есептік көрсеткіштің бес жүзге дейінгі мөлшерінде айыппұл салуға немесе сол мөлшерде түзету жұмыстарына немесе үш жүз сағатқа дейінгі мерзімге қоғамдық қызметке тартуға немесе тоқсан күнге дейінгі мерзімге белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан екі жылға дейінгі жазамен жазаланады. 2. Дәл сол әрекеттер: 1) мемлекеттік электрондық ақпараттық ресурстарға немесе мемлекеттік органдардың ақпараттық жүйелеріне қатысты; 2) адамдар тобы алдын ала келісім бойынша жүзеге асса: үш айға дейінгі мерзімге белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан айырумен екі мыңға дейінгі айлық есептік көрсеткіш мөлшерінде айыппұл салуға немесе сол мөлшердегі түзету жұмыстарына, немесе екі жылға дейінгі мерзімге бас бостандығын шектеуге не дәл сондай мерзімге бас бостандығынан айыруға жазаланады.
210-бап. Зиянды компьютерлік бағдарламалар мен бағдарламалық өнімдерді жасау, пайдалану немесе тарату	1. Ақпараттық жүйелер арқылы берілетін электрондық тасымалдағышта сақталатын ақпаратты заңсыз жою, блоктау, өзгерту, көшіру, пайдалану

	мақсатында компьютерлік бағдарламаны, бағдарламалық өнімді жасау немесе қолданыстағы бағдарламаға немесе бағдарламалық жасақтамаға түзету енгізу, компьютер жұмысын тоқтату, абоненттік құрылғы, компьютерлік бағдарлама, сондай-ақ қасақана пайдалану және (немесе) тарату осындай бағдарламаны немесе бағдарламалық өнімді жасауға тыйым салынады: кері жағдайда, үш мың айлық есептік көрсеткіш мөлшерінде айыппұл салуға немесе сол мөлшердегі түзеу жұмыстарына, немесе үш жылға дейінгі мерзімге бас бостандығын шектеуге немесе белгілі бір лауазымдарды атқаруға немесе белгілі бір қызметпен айналысу құқығынан айырумен бірдей үш жылдық мерзімге бас бостандығынан айыруға жазаланады. 2. Дәл сол әрекеттер: 1) адамдар тобының алдын ала сөз байласуы бойынша; 2) өзінің қызметтік жағдайын пайдаланатын адам; 3) мемлекеттік электрондық ақпараттық ресурстарға немесе мемлекеттік органдардың ақпараттық жүйелеріне қатысты жасалған жағдайда: үш жылдан жеті жылға дейінгі мерзімге бас бостандығын шектеуге немесе дәл сол мерзімге бас бостандығынан айыруға, белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан үш жылға дейін немес бас бостандығынан айырылады.

1.4 Веб-сайтқа төнетін қауіптер мен оның түрлері

Веб-сайтқа төнетін қауіптердің негізгі бөлігін:

1. Құпиялылық қауіпі – шабуылдаушының жабық деректерге рұқсатсыз қол жеткізу.
2. Тұтастық қаупі – деректерді рұқсатсыз бұрмалау немесе жою.

3. Қол жетімділік қатерлері – деректерге қол жетімділікті шектеу немесе бұғаттау құрайды.

Веб-сайттың ақпараттық қауіпсіздігіне негізгі қауіп-қатер көзі сыртқы бұзушылар болып табылады. Сыртқы бұзушылар - әдетте коммерциялық мүддеге негізделетін, компанияның веб-сайтына кіре алатын, зерттелетін ақпараттық жүйені білмейтін, желінің қауіпсіздігін қамтамасыз ететін жоғары білікті және әр түрлі ақпараттық жүйелерге желілік шабуылды жүзеге асыруда мол тәжірибесі бар адам.

Қауіп-қатерлері түрлері бірнеше факторлармен байланысты: бірінші кезекте, бұл веб-қосымшалардың немесе олардың компоненттерінің осалдығы. Екіншісі – сәйкестендіруді тексеру механизмдерінен. Үшінші кезекте, пайдаланушыларға жасалынатын шабуылдар, яғни клиент-сайд шабуылдарына жатады. Қауіптердің төртінші түрі – маңызды ақпаратты тарату немесе ашу. Қауіптің бесінші түрі – логикалық шабуылдар.

Веб-сайттың осалдығы, әдетте, қашықтағы сервердегі кодты орындауға әкеледі. Барлық серверлер сұраныстарды өңдеу кезінде пайдаланушы берген деректерді пайдаланады. Жиі бұл деректер динамикалық мазмұнды генерациялау үшін қолданылатын командаларды құрастырғанда қолданылады. Егер әзірлеу кезінде қауіпсіздік талаптары ескерілмесе, зиянкестер орындалатын командаларды түрлендіру мүмкіндігін алады. Мұндай осалдықты кеңінен пайдаланатын шабуыл түрі – SQL-injection болып табылады.

Пайдаланушының, қызметтің немесе қосымшаның сәйкестендіргішін тексеру үшін қолданатын немесе пайдаланушы, қызмет немесе қосымшаның әрекетті аяқтауға қажетті рұқсаты бар-жоғын анықтау үшін веб-сервер қолданатын әдістерге бағытталған шабуылдар. Мұндай шабуылдарға – bruteforce, аутентификацияны айналып өту, қауіпсіз емес парольді қалпына келтіру, сеанстың болжамды мәні немесе оны бекіту кіреді.

Сайтқа кіру кезінде пайдаланушы мен сервер арасында технологиялық және психологиялық тұрғыда сенімді байланыс орнатылады. Пайдаланушы сайттан оны заңды түрде қамтамасыз етеді деп күтеді. Сонымен қатар, пайдалнушы сайттан шабуылдар күтпейді. Осы сенімді пайдалану арқылы шабуылдаушы сервер клиенттеріне шабуыл жасау үшін түрлі әдістерді қолдана алады. Мұндай шабуылдарды, шабуылдың күрделі сценарийлерінде де (watering hole, drive by), сондай-ақ таныс - клиенттік шабуылдарда да қолдануға болады, мысалға XSS.

Ақпаратты жариялауға тікелей веб-қосымша, оның компоненттері, платформасы және құрамдас бөліктері туралы ақпарат, сондай-ақ тиісті қорғалмауынан сайттан ақпараттың сыртқа шығуы жатады. Бұл шабуылдаушыға қол жеткізуге тыйым салынған клиенттердің жеке деректеріне ашылуына алып келеді. Мұндай ақпараттың ашылуы – веб-сервердің дұрыс емес конфигурациялануынан болады.

Логикалық шабуылдар – веб-сайттың функцияларын немесе оның жұмыс істеу логикасын пайдалануға бағытталған шабуылдар түрі. Веб-сайттың логикасы - белгілі бір әрекеттерді орындау үшін бағдарламада

күтілетін процесс болып табылады. Мысалға парольді қалпына келтіру, шотты тіркеу, аукциондық сауда, электрондық коммерция жүйелеріндегі операциялар жатады. Веб-сайт нақты тапсырманы орындау үшін пайдаланушыдан бірнеше дәйекті әрекеттерді дұрыс орындауды талап етуі мүмкін. Қаскүнем бұл тетіктерді айналып өте алады немесе өз мақсаттары үшін қолдана алады. Мұндай шабуылдаң түрін – DoS шабуылы деп атайды.

1.5 Веб-сайтқа бағытталған шабуыл түрлері

Мақсатты шабуылдар - бір сайтқа немесе бір белгімен біріктірілген олардың тобына арнайы бағытталған шабуылдар(бір компанияның сайттары немесе қызметтің белгілі бір саласына жататын сайттар). Мұндай шабуылдардың қауіптілігі "Тапсырыс" сипатында жүзеге асады. Шабуылды орындаушылар әдетте веб-қосымшалардың қауіпсіздік саласында жоғары біліктілігі бар зиянкестер болады.

Мұндай шабуылдардың мақсаты әдетте теріс пиғылды бәсекелестер немесе қылмыскерлер пайда табу үшін құпия ақпарат алу болып табылады.

Мақсатсыз шабуылдар – бұл іс жүзінде "сәттілікке" жасалатын шабуылдар, ал оның құрбандары танымал, бизнес көлеміне, географиясына немесе саласына қарамастан кездейсоқ веб-сайттар болып табылады. Сайтқа мақсатсыз шабуыл жасау – бұл қаскүнемнің нақты сайтты бұзу мақсатын қоймайтын, қандай да бір талаптар бойынша іріктелген жүздеген немесе мыңдаған ресурстарды бірден шабуылдайтын веб-ресурсқа рұқсатсыз қол жеткізу әрекеті. Мысалы, сайтты басқару жүйесінің белгілі бір нұсқасында жұмыс істейтін сайттар. Мұндай шабуылдар ең аз шығынмен сайттардың ең көп санын қамтуға тырысып, "алаңдар" бойынша шабуылдайды.

Шабуылға сәтті әрекет еткен кезде қаскүнем осы пайданы алуға тырысады: хакерлік скриптті (бэкдор, веб-шелл) жүктеп, сайтқа бекіту, тағы бір әкімшіні қосу, зиянды кодты енгізу немесе деректер базасынан қажетті ақпаратты алу.

Мақсатты шабуылдар - жасырын түрде жүзеге асырылғандықтан, әдетте олар өз мақсаттарына жетеді. Мақсатсыз шабуылдар айтарлықтай «шулы» және олар көбіне өз мақсаттарына жете бермейді, бірақ соған қарамастан олар веб-ресурстың иесіне көптеген проблемалар тудыруы мүмкін.

1.6 Себебі мен салдары

Бірінші кезекте бұл сайттың жұмысқа қабілеттілігіне қауіп төндіреді. Екіншісі – пайдаланушы мәліметтерінің сақталуы. Осы себептерден компанияның қаржылық және бедел шығындарының — қисынды салдары туындайды.

Хакерлер сіздің сайтыңызды басқа ресурстарға шабуыл жасау үшін, анықтамалық көпір ретінде, спам жіберу немесе DoS шабуылдарын жасау үшін пайдаланады. Сіздің сайтыңызды іздеу жүйелері мен браузерлерде

пайда болуын бұғаттайды. Мұндай шабуыл пайдаланушылардың жоғалуына әкеп соқтырады. Сондай-ақ, барлық осы шабуылдар сайт пайдаланушыларын одан әрі "жұқтыруға" бағытталуы мүмкін, мысалы, браузерлер осалдықтарын және олардың компоненттерін пайдалану құралдарын эксплоит — пакеттері арқылы, оның ішінде шабуылдың әлеуметтік-техникалық векторларын қолдана отырып зақым келтіре алады.

Веб-қосымшаға шабуылдардың таралуы екі негізгі факторлармен байланысты: сайттың қауіпсіздігіне немқұрайлылық қатынас және әлеуетті зиянкестердің кіру шегі төмен.

Көптеген жағдайларда сайттар анықтаудың, бақылаудың және қорғаудың арнайы құралдарын пайдаланбайды және жауапты қызметкерлер жоқ, сондықтан сайттың қауіпсіздігіне төнетін қауіптер туралы хабардар болмайды. Кодтың сапасына және веб-сайттың қауіпсіз конфигурациясына аз көңіл бөлінеді.

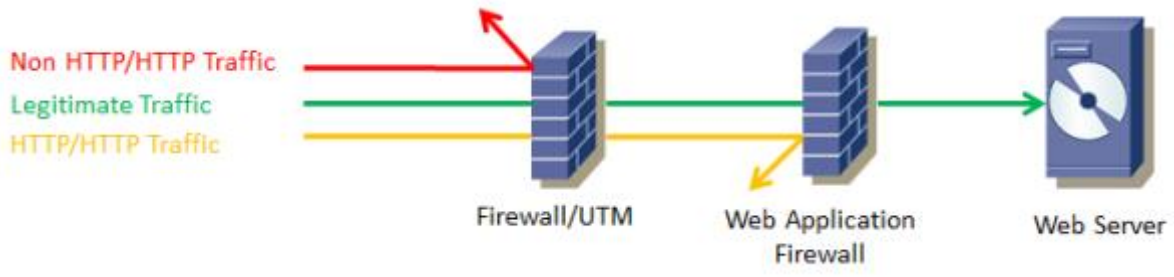
Веб-қосымшалардың қауіпсіздік бағдарламалары мен сканерлерін тарату – әлеуетті зиянкестердің кіру шегінің төмен болуына себепші болады. Ал көптеген коммюнити және "хакерлерге" арналған форумдарда барлық тілек білдірушілер арасында шабуыл техникаларының іске асу жолдары мен таралуына ықпал етеді. Сондай-ақ бұған жаңа осалдықтарды немесе шабуылдардың техникалық аспектілерін табу туралы кең және жедел жария ету себепші болады.

1.7 Веб-сайтты қорғау әдістері

Сайтты қорғауды қамтамасыз ету үшін оңтайлы шешім Web Application Firewall — сайттарды зиянкестердің шабуылдарынан тиімді қорғауға мүмкіндік беретін қолданбалы деңгейдегі желіаралық экранды қолдану болып табылады.

Web Application Firewall – бұл HTTP-пакеттерді өңдей отырып, сервер мен клиенттің өзара әрекеттесуіне белгілі бір ережелер жиынтығын қоятын арнайы механизм. Негізінде жұмыс істеу қағидасы желіаралық экран тәрізді, яғни сырттан келіп түсетін барлық деректерді бақылайды. WAF ережелер жиынтығына сүйене отырып, пайдаланушының белсенділік белгілері бойынша шабуылдар фактісін анықтайды.

WAF клиенттен келетін мәліметтерді талдай отырып және заңсыз сұрауларды алып тастай отырып, ашық прокси режимде жұмыс істейді, яғни:



1.3 сурет – WAF-тың жұмыс істеу механизмі

Web Application Firewall орнатқаннан кейін оны мақсатты веб-қосымшасы үшін конфигурациялау керек. CMS типіне және түріне байланысты, веб-қосымшаны ескеретін сүзбе параметрлері мен ережелері қосылады және қорғаныс құралы сілтеме үлгілерін жинау үшін жаттығу режиміне енгізіледі.

Web Application Firewall қолдану тиімділігі бірнеше факторлардан тұрады:

- Парольдерді болжау мен анықтауға арналған құрылғыларды бұғаттау;
- Шабуылдар туралы ақпараттандырудың ыңғайлы қызметі;
- Жалған іске қосылудың төмен мөлшері;
- Қарапайым интеграция;
- WAF өзін-өзі қорғау;

Веб-сайттқа қорғаныс ұйымдастырудың тағы бір түрі ол – HTTPS хаттамасы

HTTPS – бұл қолданушыдан серверге және кері ақпаратты сенімді шифрлауға мүмкіндік беретін кәдімгі HTTP үшін қорғаныс қабығы. Мұндай шифрлау деректердің ағып кетуіне жол бермейді, яғни сайтты бұзудан қорғайды.

HTTPS хаттамасына өту барлық сайттар үшін қатаң талап емес. Әрине, егер сайт клиенттердің төлем деректерімен немесе кез келген басқа да жеке ақпаратпен жұмыс істесе, мұндай хаттама міндетті түрде орнатылуы тиіс. Барлық басқа жағдайларда HTTPS хаттамасын орнату, не орнатпауын сайт иесі шешеді. Алайда, спамды тарату, күмәнді мазмұндағы сайттарға автоматты түрде өту немесе тіпті толық жою жағдайындағы қиындықтар кез келген сайтқа қауіп төндіреді. Тәжерибе көрсеткендей, HTTPS хаттамасын қолданатын сайттардың пайдаланушылары өздерінің дерек қорларын сенімді түрде тапсырады.

Жоғарыда айтылғандай, деректерді жіберетін HTTP протоколы іс жүзінде ештеңемен қорғалмайды және ақпарат хакерлер үшін оңай олжа бола алады. Ақпараттың ағып кету мүмкіндігін болдырмау үшін, SSL / TLS криптографиялық жүйесін қолдана отырып, HTTPS протоколы 1994 жылы құрылды. Ол барлық жіберілген деректерді шифрлайды және қорғалмаған арналар арқылы қауіпсіз байланыс орнатуға мүмкіндік береді.

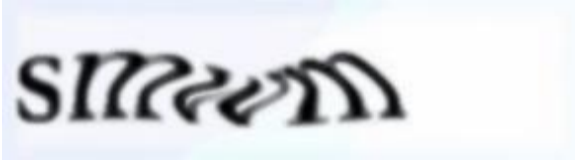
Веб-сайтқа желі арасында қорғаныс ұйымдастырумен ғана тоқталмай спамдардан да қорғану қажет.

Сайтты спамдардан қорғау үшін, бірінші кезекте – қонақтар кітабындағы жазба қалдыру формасы мен түсініктеме формаларын дұрыс орнату керек. Мысалы, форманың барлық жолдары міндетті толтырылатынын, жіберушінің электрондық поштасының мекен-жайы тиісті ережелерге сай толтырылғанын тексеру.

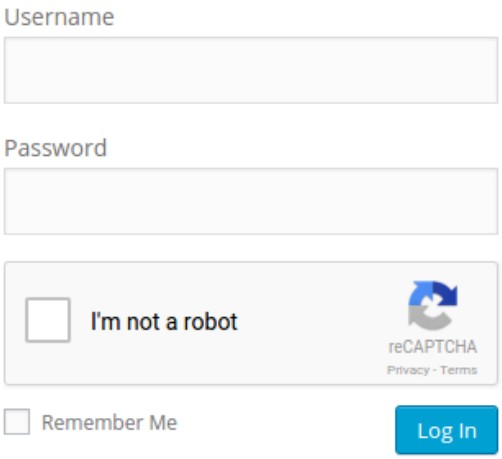
Егер сайтта пікір қалдырушылар саны көп болмаса, оны қолмен қорғауға болады. Мұны істеу үшін, әдетте, жариялаудың алдында барлық пікірлерді әкімші спам сілтемелерін бар-жоғын модерацияланудан өтекізеді. Спам сілтемелері табылмаған жағдайда әкімші оны веб-парақшаға

жариялайды. Мұндай әдіс пікір қалдырушылар саны өте көп болған жағдайда өз жұмысын тоқтатады, ал оның орнына спамдардан автоматтандырылған қорғану әдісі, яғни – капча (CAPTCHA) келеді.

CAPTCHA (Толығымен автоматтандырылған адаммен компьютерді айырып тануға көпшілікке арналған тест Тьюринг) - бұл компьютерлерді адамдардан ажырататын арнайы тесттің атауы. Нағыз адам тестте ұсынылған мәселені оңай шеше алады, бірақ компьютердің оған шамасы жетпейді. Көбінесе, CAPTCHA сәл бұрмаланған әріптер (1.5 – Сурет) немесе сандармен суретке ұқсайды. Көру қабілеті төмен адамдар үшін дыбыстық CAPTCHA ұсынылады. Барлық капчтар арасында кеңінен танымал және қолданылатындары ол – reCAPTCHA. reCAPTCHA адам мен компьютерді тану үшін ең сенімді тест болып саналады, алайда оны дұрыс өту кейбір кезде қарапайым адамдарға қиын, сондықтан ол жиі пайдаланушылардың наразылығын тудырады. Басқа капчтар аз күрделі, бірақ олардың қорғау деңгейлері сәл төмен болып келеді.



1.4 сурет – Бұрмаланған әріптер



1.5 сурет – WordPress платформасындағы reCAPTCHA

Түсініктеме формасына және қонақ кітаптарына капчаны орнату спам-түсініктемелер мен спам-посттарды алу қаупін айтарлықтай төмендетуге көмектеседі. Бірақ бұл сайтты спамнан қорғаудың жалғыз тәсілі емес. Сондай-ақ, осы мақсатта спамның автоматты түсініктемелерін мәтіндегі белгілі бір кілт сөздеріне қарай тексеру, referer параметрі бойынша сүзу, нысанды толтыру уақытын тексеру және т.б. әдістер арқылы іздеуге мүмкіндік беретін спамға қарсы CMS платформасында плагиндер қолданылады.

2 Веб-сайтты әзірлеуге қолданылған технологиялар мен құрал-жабдықтар

2.1 Open Server

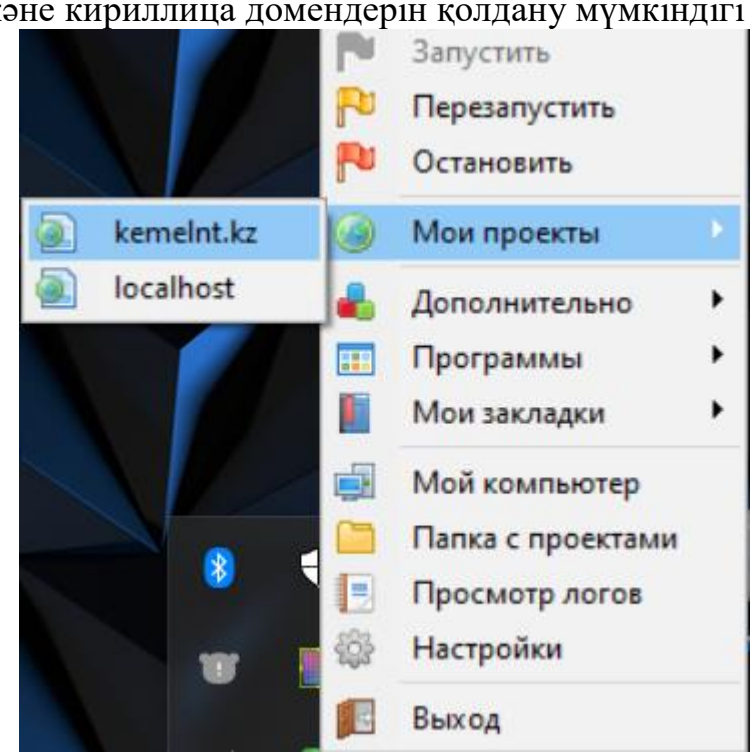
Open Server Panel - бұл веб-әзірлеушілердің ұсыныстары мен тілектері негізінде арнайы жасалған портативті сервер платформасы және бағдарламалық жасақтама ортасы болып табылады.

Бағдарламалық кешенде серверлік бағдарламалық қамтамасыз етудің бай жиынтығы бар және ыңғайлы, көп функционалды, жақсы ойластырылған интерфейсі бар, сондай-ақ компоненттерді басқаруға және конфигурациялауға арналған керемет мүмкіндіктермен жасақталған платформа болып саналады. Платформа веб-жобаларды әзірлеу, жөндеу және тестілеу, сондай-ақ жергілікті желілерде веб-қызметтерді ұсыну үшін кеңінен қолданылады.

Алғашқыда, кешен құрамына кіретін бағдарламалық өнімдер бір-бірімен жұмыс істеу үшін арнайы әзірленбеген болса да, мұндай байланыс Windows пайдаланушылары арасында өте танымал болды, себебі Open Server платформасы тегін бағдарламалық жасақтама бола тұра, серверлері Linux деңгейінде жұмыс істеді.

Open Server-дің басқа серверлік платформалардан ерекшелігі:

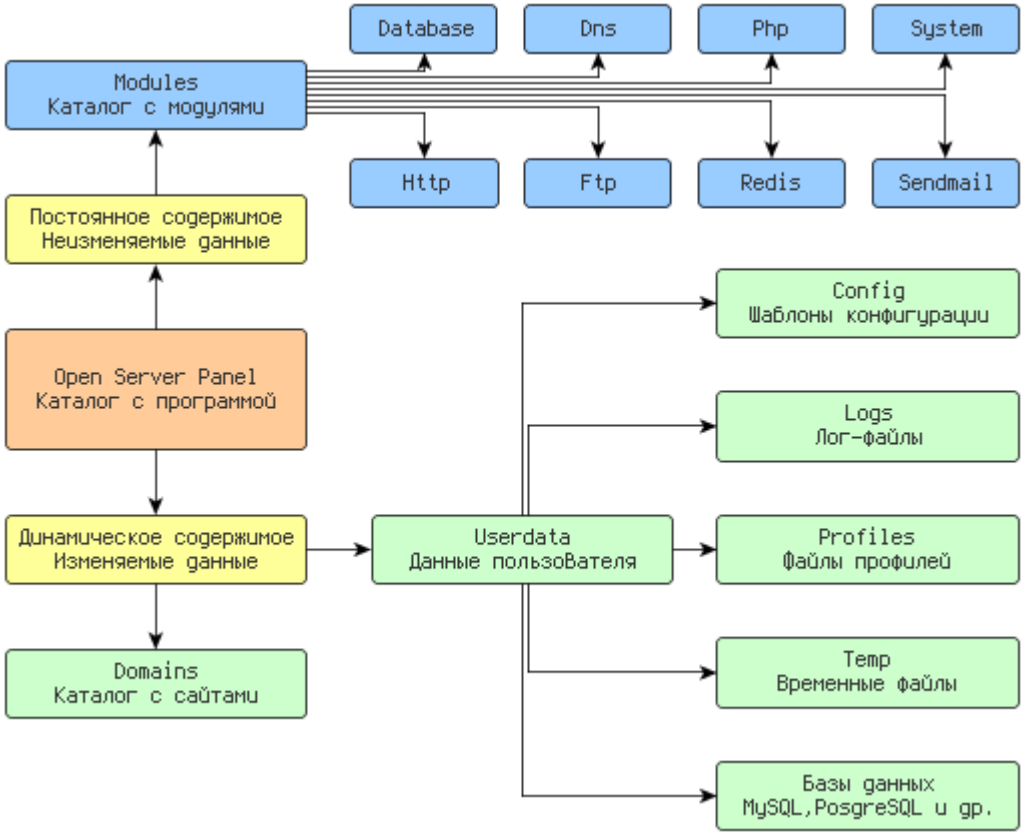
- CMS мазмұнды басқару жүйесімен үйлесімділігі;
- Нақты уақыт режимінде барлық компоненттердің журналдарын қарау;
- HTTP, ДББЖ және PHP модульдерін кез келген комбинацияда таңдау;
- SSL және кириллица домендерін қолдану мүмкіндігі және т.б.;



2.1 сурет – «KEMEL-NT» веб-сайты

Open Server Panel серверлік платформасының логикалық құрылымы (2.2 сурет) 2 бөліктен тұрады:

1. Динамикалық. Бұл бөлікте Open Server Panel-дің өзгеретін деректері сақталады. Мысалға, веб-сайт үшін мұнда: пайдаланушылардың деректері және сайттың тізімдерінен тұрады



2.2 сурет – Open Server Panel архитектурасының логикалық құрылымы

2.2 Content Management System

Content Management System – бұл веб-ресурстың құрылымы мен мазмұнын басқаруға мүмкіндік беретін бағдарламалар жиынтығы. Кәсіби жаргонда CMS «қозғалтқыш» деп те аталады.

Бұрын сайттардың көпшілігі статикалық сипатта болды және олардың мазмұнын қолмен өзгертуден басқа мүмкіндік болмайтын, бірақ қазір жобалардың даму динамикасы өзгерістерге тез жауап беруге және оларды қысқа уақыт мерзімінде максималды тиімділікпен іске асыруға дайын болуды талап етеді.

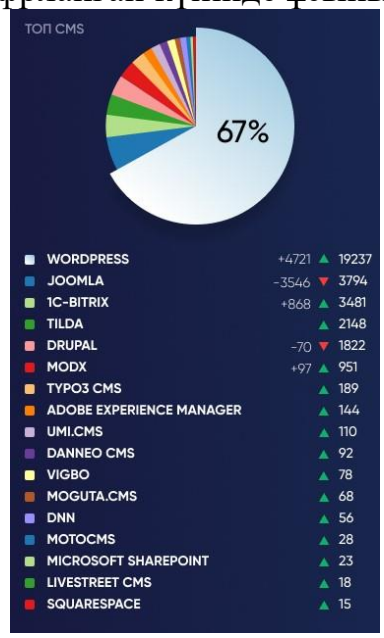
Сервер бөлігі деректер базасы мен веб-сайттың функционалдығынан тұрады. Мазмұн деректер базасында сақталады және пайдаланушы веб-бетті сұрағанда кезде ішкі интерфейстен сыртқы интерфейске жіберіледі. Веб-сайттың ішкі функционалдығы PHP, Python, JavaScript және т.б. танымал бағдарламалау тілдерінде жазылған.

CMS-тің негізгі артықшылықтары:

- Жұмыста нақты мәселені шешудің ең тиімді құралы қолданылады (сайттың түріне және оның жұмысына қойылатын талаптарға байланысты, оңтайлы CMS таңдалады);

- CMS пайдалану сайттың иесіне сайт бөлімдерін өз бетінше құруға және жоюға, сырттан шақырылған маманының қатысуынсыз әртүрлі ақпаратты өңдеуге мүмкіндік береді – бұл статикалық сайттардан артықшылығының бірі;
- Сайт жұмысы үнемі көптеген пайдаланушымен тестіленеді, ал табылған қателер мен осалдықтар жедел түрде жойылады, бұл ретте сайт ең озық және тексерілген техникалық шешімдерде жұмыс істейді;

Қазіргі таңда CMS мазмұнды басқару жүйесінің көптеген түрлері бар. Мысалғы, кейбір жүйелер тек нақты міндеттерді шешуге бағытталған (блогтар жүргізу, Интернет дүкендер, форумдар), басқалары әмбебап болып табылады және кез келген нәрсені әзірлеу үшін жобалаудың және бағдарламалаудың ыңғайлы ортасын ұсынады. CMS бөлігі көптеген функционалдық блоктардан және модульдерден тұрады, кейбірі монолитті, бөлінбейтін, сондай-ақ шифрланған күйінде ұсынылады.



2.3 сурет – Қазнеттегі танымал CMS платформалар

2.3 WordPress

WordPress – бұл өзіңіздің веб-сайтты құруға арналған, веб-қосымшаның негізінде құрастырылған заманауи жүйе. Бұл жүйе PHP бағдарламалау тілінде жүзеге асырылады, ал деректер базасы ретінде MySQL тілі қолданылады. WordPress плагиндер көмегімен өзінің мүмкішілігін арттыра отырып түрлі пайдалы құралдармен жабдықталған және ашық кодты көзін пайдаланады. WordPress әмбебап платформалар түріне жатқызуға болады, себебі қарапайым блогтардан бастап, күрделі жаңалықтар ресурстарына дейін қосымшаларды жасауға болады.

Сонымен, WordPress қозғалтқышының функционалдық мүмкіндіктерін қарастырайық:

1. Тұрақты парақтарды жасауға, жоюға және өңдеуге мүмкіндік береді (мысалы, «Компания туралы», «Контактілер», және т.б. парақтар).

2. Жазбаларды (жарияланымдарды) жасауға, жоюға және өңдеуге мүмкіндік береді.

3. Түсініктемелермен жұмыс істеудің кең мүмкіндіктері (ағаш тәрізді пішімді немесе бір беттегі ең көп сан және т.б. параметрлерді қосу немесе өшіру).

4. Таңбаларды, айдарларды, RSS және іздеуді қолдау.

5. Екі режимде жұмыс істейтін WYSIWYG (What You See Is What You Get – не көресің, соны аласың) тамаша мәтіндік редакторы: визуалды және html форматында.

6. Фотосуреттер мен бейнелердің онлайн редакторы, кесу, айналдыру, масштабтау және т. б. өңдеу құралдары.

7. Стандартты емес функцияларды қосуға мүмкіндік беретін әртүрлі плагиндер мен виджеттердің үлкен жиынтығы.

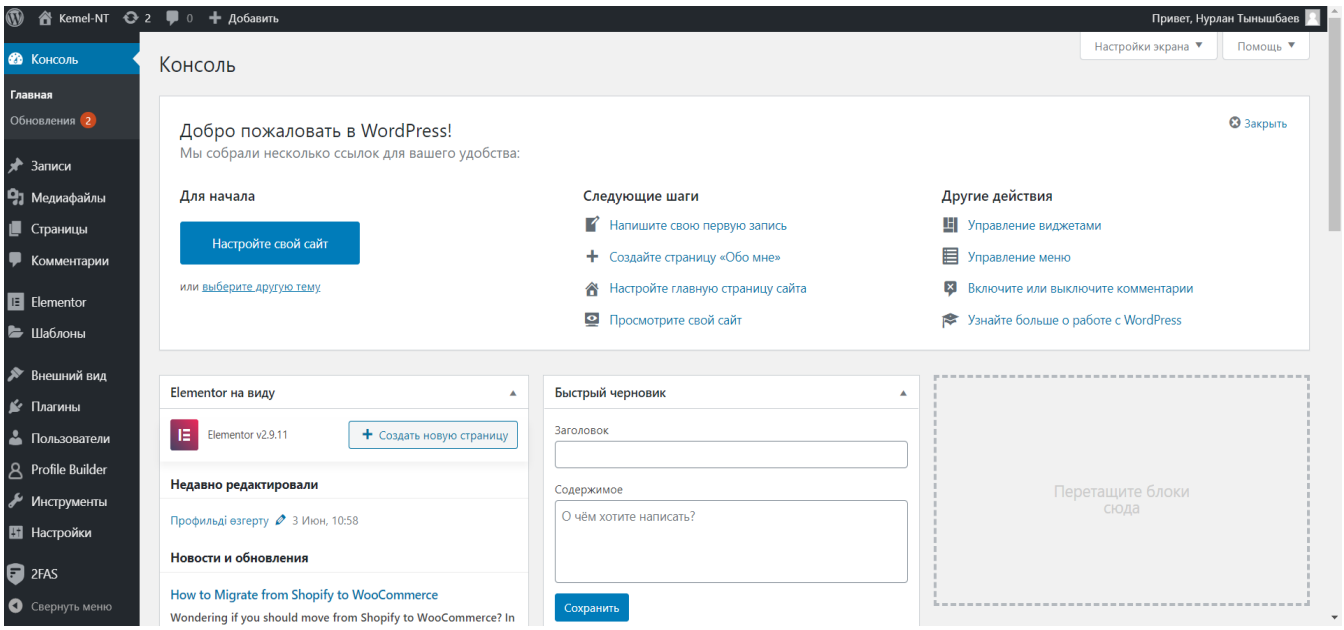
Жоғарыда көрсетілген мүмкіндіктерімен қоса, WordPress платформасының басқаларға қарағанда 5 артықшылығын атап кетуге болады:

- Ақысыз. WordPress – бұл тегін жүйе. Өз блогыңызды немесе шағын жобаны жасағысы келетін жаңа әзірлеуші үшін бұл маңызды дәлел және үлкен артықшылық.
- Кроссплатформалы. WordPress веб-сайтыңызға (серверге) тікелей орнатылады және қолданылады. Компьютерге артық программаларды орнатуды қажет етпейді. Бұл кез-келген операциялық жүйеден және кез-келген компьютерден сайтты басқаруға болатындығын білдіреді. Жалғыз шарт - Ғаламторға қосылу.
- Кірістірілген редакторы бар.
- Танымалдылығы. WordPress-әлемдегі ең танымал сайт мазмұнын басқару жүйесі. Ресми статистикаға сәйкес, басқа бәсекелестердің арасында WordPress нарығының үлесі 55% - дан асады. Әлемдегі 58 миллионнан астам сайт WordPress-те жұмыс істейді. Әлемдегі әрбір 7-ші сайт WordPress-те құрылған және жұмыс істейді.

WordPress негізгі артықшылықтарының тізімін қосымша мүмкіндіктермен толықтыруға болады:

- озық функционалға және икемділікке ие сапалы ақылы тақырыптардың үлкен кітапханасының болуы;
- ресурстардың оқылуы мен трафигін жақсарту үшін виджеттер мен әлеуметтік плагиндердің қол жетімділігі;
- жүйенің сенімділігі мен қауіпсіздігі;
- түрлі құралдар көмегімен веб-сайтты өңдеу мүмкіншілігі;
- әмбебап блоктардың болуы;
- пайдаланушыларды басқару құқығының болуы.

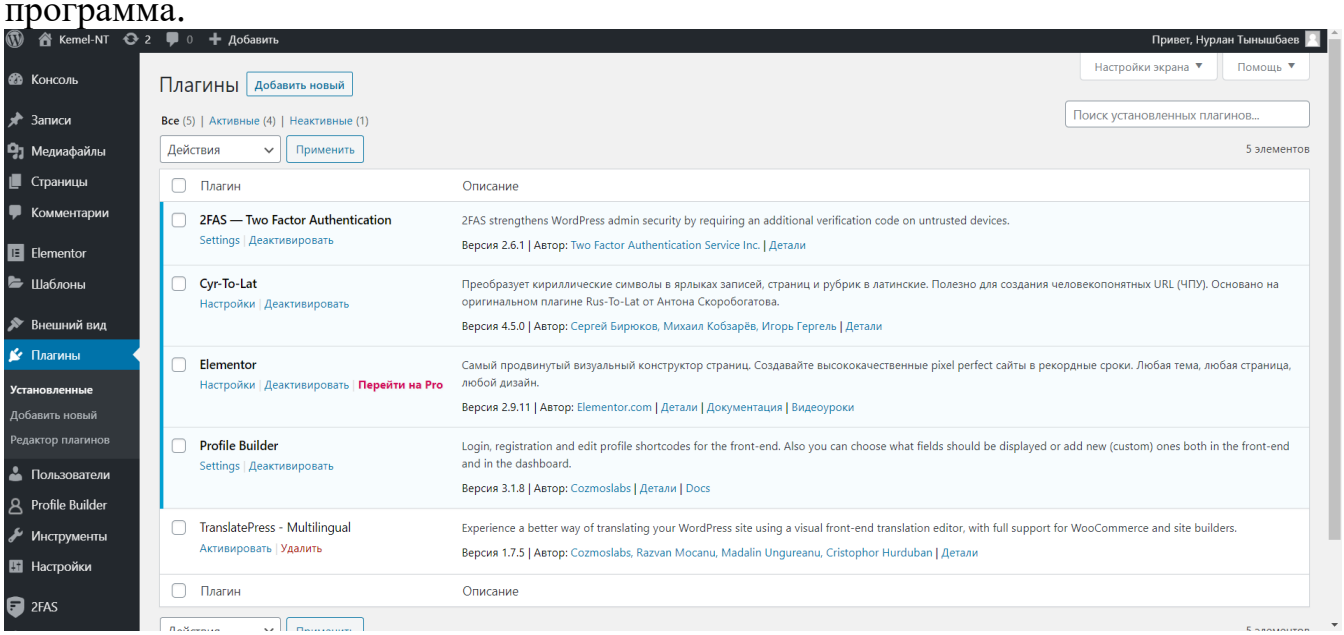
WordPress платформасының консольінде (2.4 сурет) алдымен сайтты орнатып, бастапқы параметрлерімен, яғни жазбалар, виджеттер, мәзірді басқару сынды т. б. құралдарымен жұмыс істеу сұрайды.



2.4 сурет – WordPress платформасының консолі

Сайт әзірлеу барысында қолданылған плагиндер тізімі 2.5 суретте көрсетілген, олар:

1. 2FAS. Бұл қос факторлық аутентификацияны жүзеге асыруға арналған арнайы бағдарлама. Бұл бағдарламаның ерекшелігі жасырын код мобильді қосымшада орнатылған бағдарламалық жасақтамада болады.
2. CyrToLat - хабарламалардың, парақтардың және тақырыптардың жапсырмаларындағы кириллица таңбаларын латынға айналдырады. Бұл плагин пайдаланушы URL мекенжайларды оқу үшін қолданылады.
3. Elementor. Ең озық көрнекі веб-парақша құрастырушы.
4. Aksimet – бұл спамды түсініктемелерден, хабарлау тетігінен (Trackback) және байланыс нысаны туралы хабарламалардан сүзгілейтін программа.

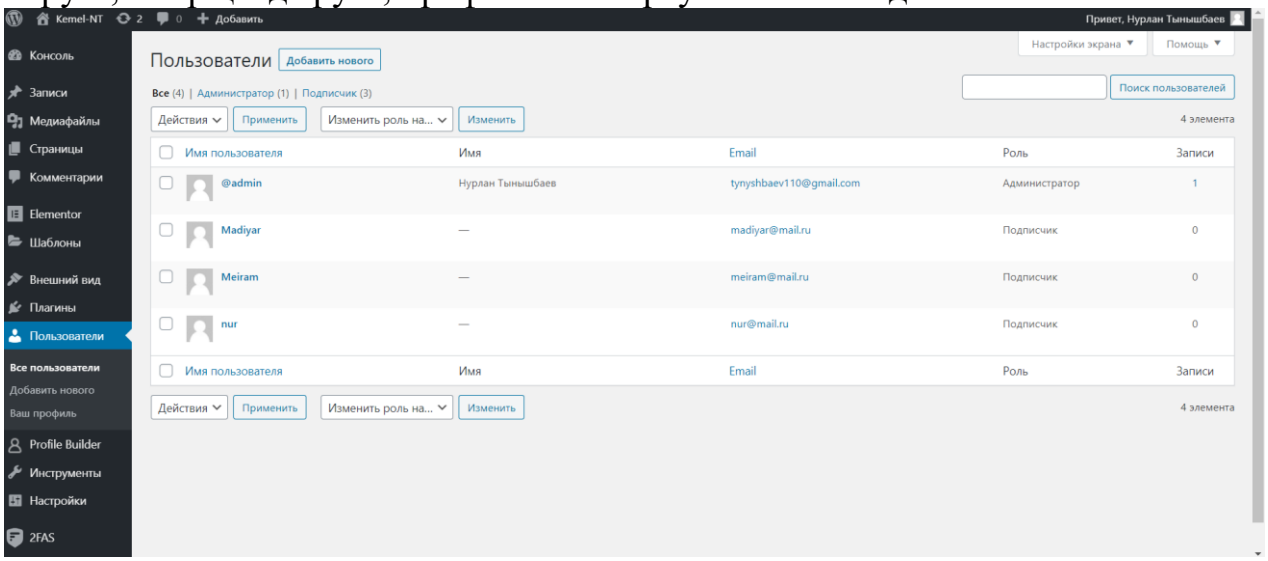


2.5 сурет – Веб-сайтты әзірлеу барысында қолданылған плагиндер

Веб-сайтта екі пайдаланушы рөлі бар (2.6 сурет), олар:

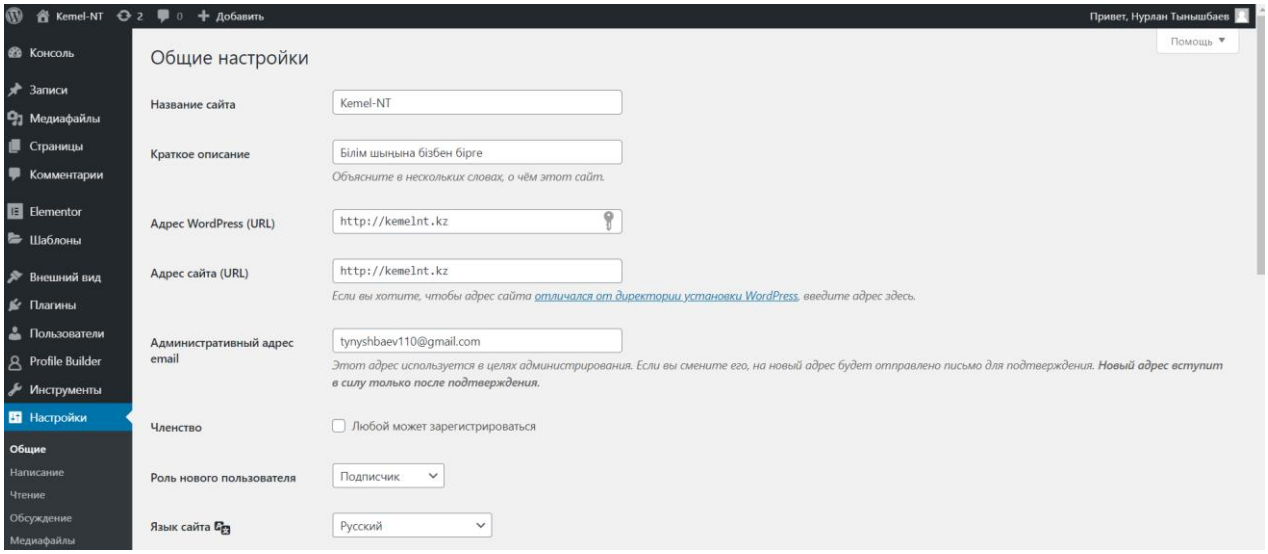
1. Әкімші. Бұл веб-сайтты әзірлеуші адам.

2. Оқушылар. Әкімшіден кейін әрбір сайтқа тіркелуші оқушылар болады. Оқушының мүмкіншілігі веб-сайтқа тіркелуге, бейнероликтерді көруге, пікір қалдыруға, профильін өзгертуге ғана болады.



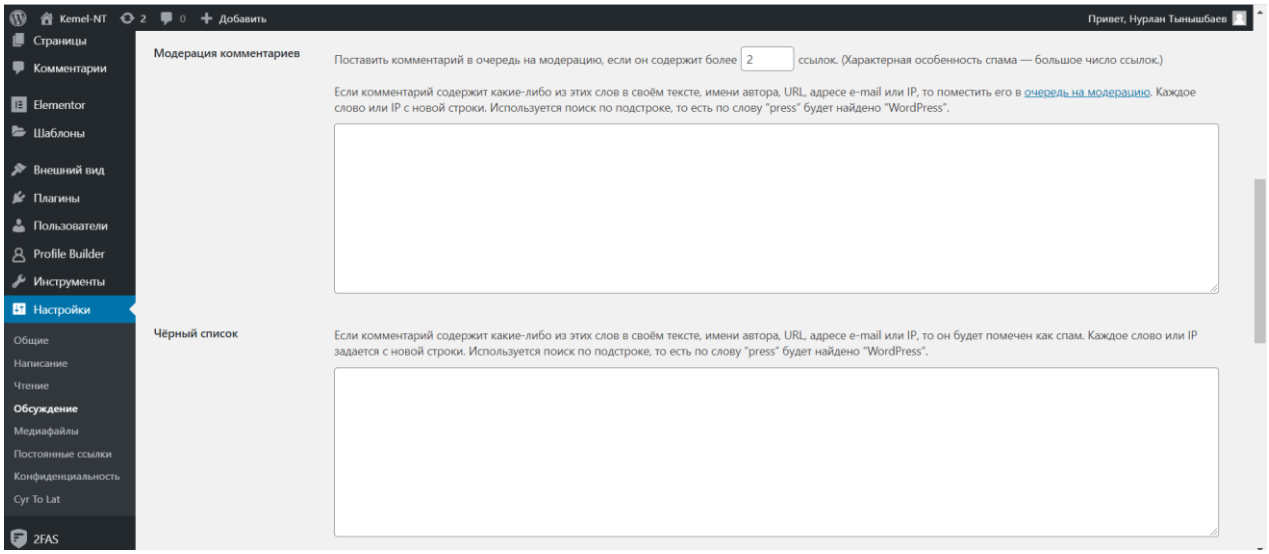
2.6 сурет – Веб-сайтты пайдаланушылар және олардың рөлдері

WordPress-тің жалпы параметрлерінде (2.7 сурет) веб-сайттың атауы және сайт жайлы қысқаша мағұлмат, URL мекен-жайы, әкімшінің электронды поштасы және т. б. параметірін баптауға болады.



2.7 сурет – Веб-сайттың жалпы параметрлері

2.8 суретте пайдаланушылардың қалдырған пікірлерін тексеруден өткізуге арналған модерацияланудың параметрі берілген. Мысалға, веб-сайтта пайдаланушы екі немесе одан да көп сілтеме қалдырған жағдайда автоматты түрде әкімшінің тексерісіне түседі, егер пайдаланушыдан зиян келтіретін сілтемелер табылмаса оны сайтқа шығарады, табылған жағдайда әкімші пікірді жойып пайдаланушыны блокқа түсіреді.



2.8 сурет – Модерацияланудың параметрлері

2.4 phpMyAdmin

phpMyAdmin – бұл PHP бағдарламалау тілінде жазылған және MySQL серверін бүкіләлемдік желі арқылы басқаруға арналған бағдарлама. phpMyAdmin MySQL-дің кең жиынтығын қолдайды. Ең жиі қолданылатын операцияларға пайдаланушы интерфейсі қолдау көрсету арқылы (дерекқорларды, кестелерді, өрістерді, байланыстарды, индекстерді, пайдаланушыларды, құқықтарды басқару және т.б.) өзгерістер еңгізуге және бір мезгілде кез келген SQL сұрауды тікелей орындауға болады.

phpMyAdmin бағдарламасында жаңа деректер базасын құруға, сақтық көшірме жасауға және т.б. қызметтерді жасауға болады. PhpMyAdmin әрбір хостингте орнатылған және жергілікті Open Server Panel серверінің стандартты конфигурациясына кіреді.

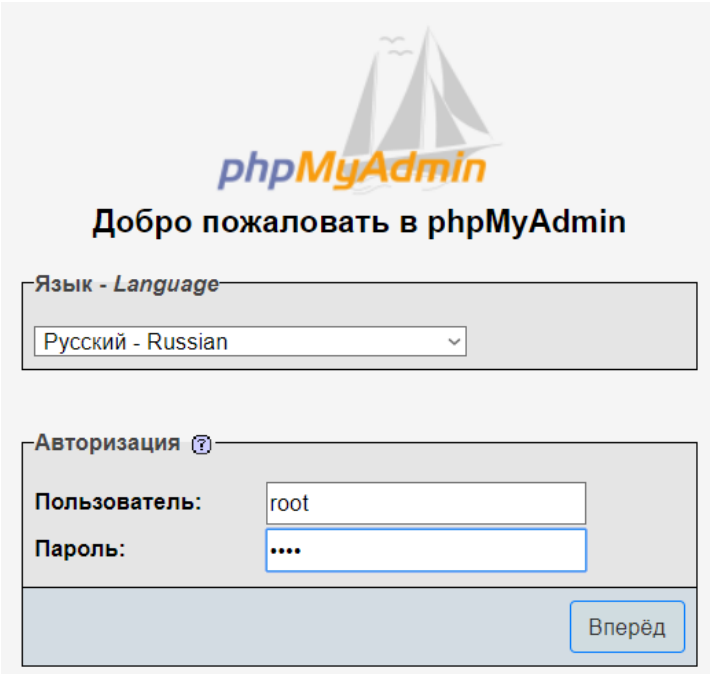
phpMyAdmin бағдарламасының мүмкіндіктері:

1. Түсінікті веб-интерфейс.
2. MySQL дерекқорларды базасын басқару жүйесі арқылы көптеген функцияларынның қолдауы:
   - мәліметтер базасын, кестелерді, көріністерді және индекстерді қарау және жою;
   - мәліметтер базасын, кестелерді, өрістерді және индекстерді құру, көшіру, жою, атын өзгерту және өзгерту;
   - серверді, дерекқорларды және кестелерді серверді теңшеу жөніндегі кеңестерге жүгіне отырып басқару;
   - SQL-дің кез-келген мәлімдемесін, соның ішінде пакеттік сұраныстарды орындау, өңдеу және сақтау;
   - MySQL пайдаланушыларын және олардың артықшылықтарын басқару;
   - сақталған процедуралармен және триггерлермен жұмыс.
3. Бірнеше серверлерді басқару.
4. Деректер базасындағы жаһандық немесе ішінара іздеу.

5. BLOB деректерді сурет немесе жүктеу сілтемесі түрінде көрсету сияқты арналған функциялар жиынтығын пайдалана отырып, деректерді кез келген пішімге түрлендіру.

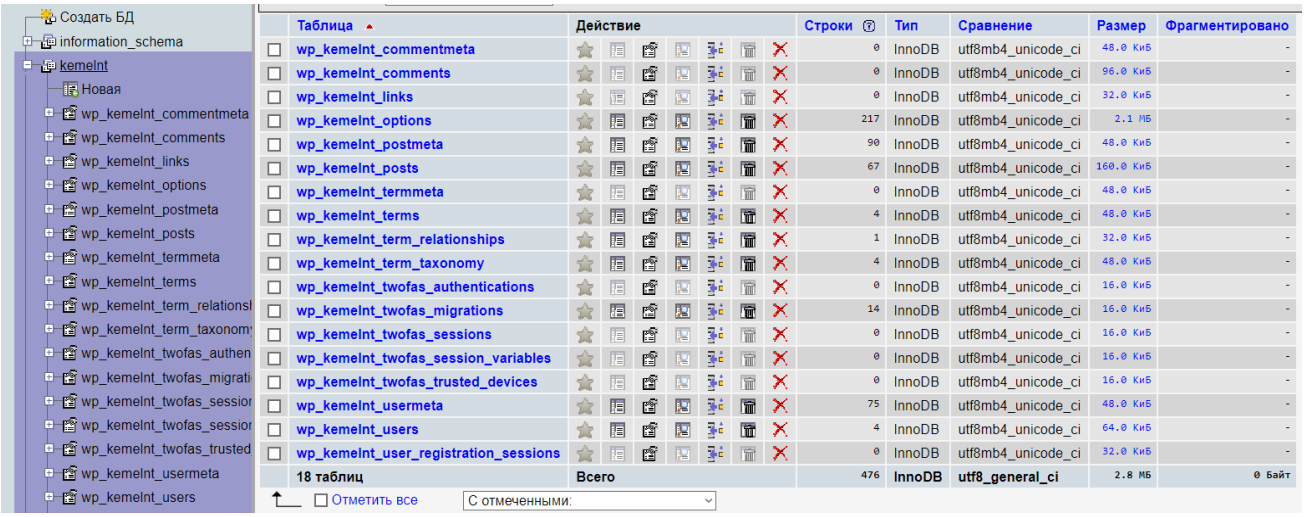
6. PDF түрінде деректер қорының көрнекі схемаларын жасау.

7. Дерекқорға түскен құпиясөзді MD5 128-биттік хэштеу алгоритмі арқылы жасыру және т.б.



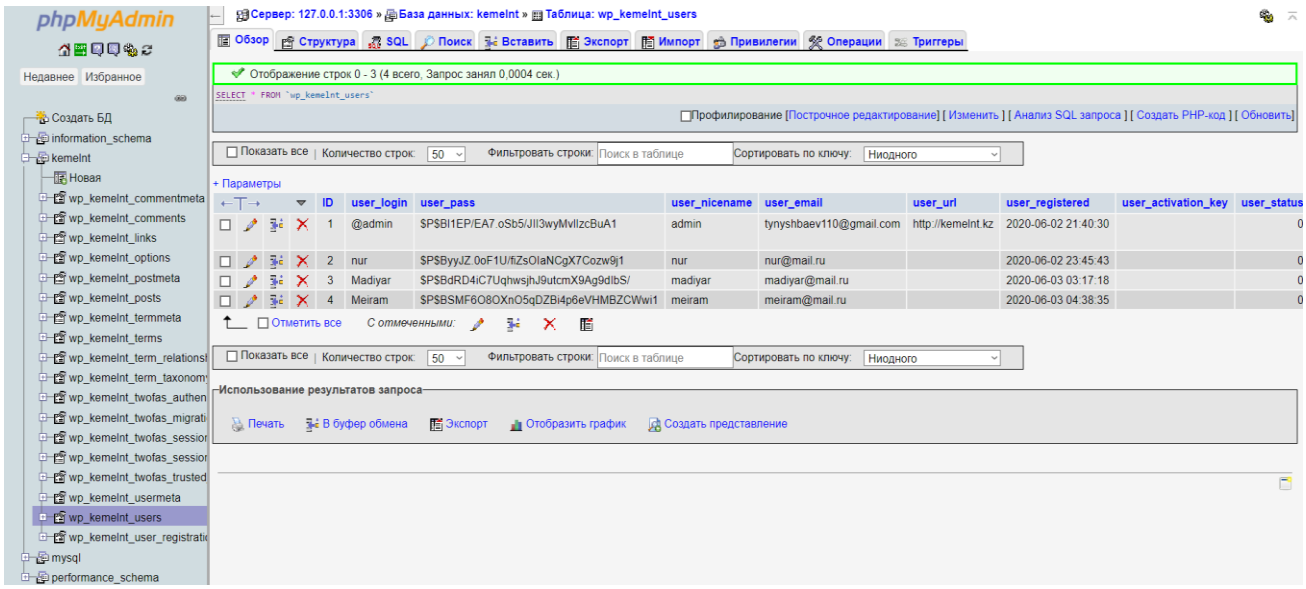
2.9 сурет – phpMyAdmin бағдарламасына кіру

«Kemel-NT» веб-сайтының дерекқорлар базасында (2.10 сурет) жаңа тіркелген пайдаланушылар, сайтқа енгізілген ақпараттар, қалдырылған пікірлер мен түсініктемелер және т.б кестелер сақталған.



2.10 сурет – «Kemel-NT» веб-сайтының дерекқорлар базасы

Мысалға, «wp_kemelnt_users» кестесінде (2.11 сурет) дерекқорлар базасына тіркелген пайдаланушылар жайлы ақпаратты алуға болады. Мұнда тіркелушінің логині, паролі, аты-жөні, тіркелген уақытысы сақталады.



2.11 сурет – Дерекқорлар базасына тіркелген пайдаланушылар

2.5 Сәйкестендіру. Аутентификация. Авторландыру

Веб-сайтқа тіркелу 3 кезеңнен өтеді (2.12 сурет), олар – сәйкестендіру, аутентификация және авторланыдырудан тұрады

Сәйкестендіру - пайдаланушыны оның сәйкестендіргіші (аты) арқылы тану процедурасы. Бұл функция негізінен пайдаланушы желіге кіруге әрекет жасағанда орындалады. Пайдаланушы жүйеге сұрау бойынша өзінің идентификаторын айтады, ал жүйе оның дерекқорды бар-жоғын тексереді тексереді.

Аутентификация – мәлімделген пайдаланушының, процестің немесе құрылғының түпнұсқалығын тексеру рәсімі. Бұл тексеру пайдаланушы (процесс немесе құрылғы) өзін жариялайтын адам екеніне сенімді көз жеткізуге мүмкіндік береді. Аутентификация жүргізу кезінде тексеруші тарап тексерілетін тараптың түпнұсқалығына көз жеткізеді, бұл ретте тексерілетін тарап ақпарат алмасу процесіне белсенді қатысады. Әдетте пайдаланушы жүйеге бірегей, басқа пайдаланушыларға белгісіз өзі туралы ақпаратты (мысалы, парольмен) енгізе отырып, өзінің сәйкестендірлілуін растайды.

Сәйкестендіру және аутентификация субъектілердің (пайдаланушылардың) түпнұсқалығын тану және тексеруде өзара байланысты процестер болып табылады. Жүйе ресурстарына нақты пайдаланушыға немесе процеске қол жеткізуге рұқсат етуі осы екі тексеріс анықтайды. Субъектіні сәйкестендіргеннен және аутентификациялағаннан кейін оны авторландырылуы орындалады.

Авторландыру — субъектіге осы жүйеде белгілі бір өкілеттіктер мен ресурстарды беру рәсімі. Басқаша айтқанда, авторландыру субъектінің әрекет аясын және оған қол жетімді ресурстарды белгілейді. Егер жүйе авторланбаған пайдаланушыны авторланған пайдаланушыдан ажырата алмаса, онда ақпараттың құпиялылығы мен тұтастығы бұзылуы мүмкін.

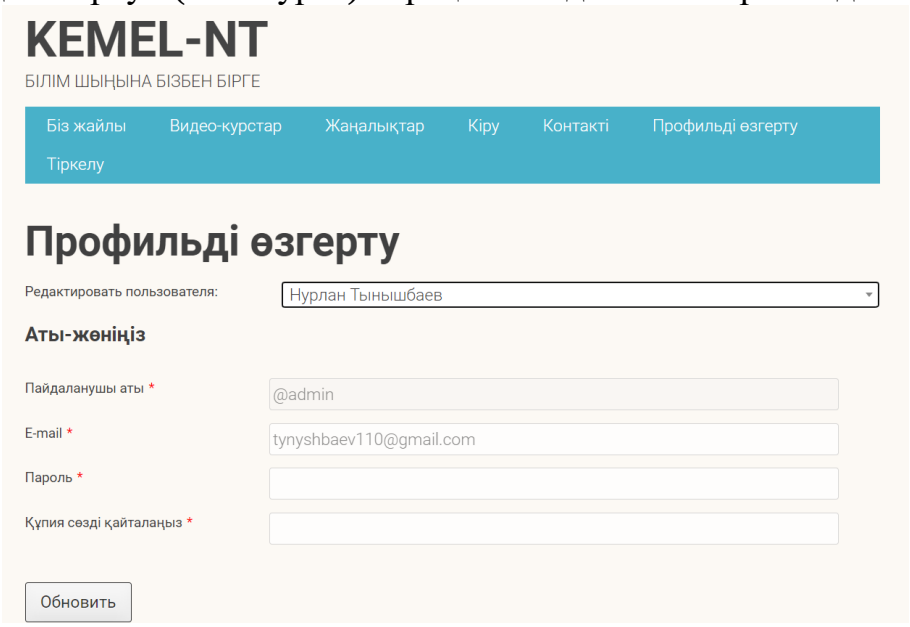
2.12 сурет – Веб-сайтқа сәтті тіркелудің кезеңдері

2.6 Аккаунт

Аккаунт – «есеп жазбасы» немесе «тіркелгі» деген мағынандан шыққан және ол қандай да бір сайтта немесе интернет сервисінде енгізетін және сақтайтын пайдаланушы туралы деректер жиынтығын білдіреді. Басқаша айтқанда, аккаунт – бұл пайдаланушы қажетті веб-сайтқа тіркелу үшін толтыратын интернет-төлқұжат. Тіркелгіні құру кезінде пайдаланушы өзінің электрондық поштасын, логині мен паролін енгізеді.

Веб-сайттың әкімшілігі пайдаланушының жеке деректерін жария етпеу міндетін өз мойнына алады. Өз кезегінде пайдаланушыдан тіл тигізуді және нормативтік емес лексиканы қолданбауды, сондай-ақ сайт немесе сервис беттерінде ұлтаралық алауыздықты қоздырмауды талап етеді.

Егер пайдаланушы электронды пошатсын өзгерткен жағдайда немес басқа да түрлі себептермен өзінің профилын өзгерткісі келсе, онда оны «профильді өзгерту» (2.13 сурет) парақшасында іске асыра алады.

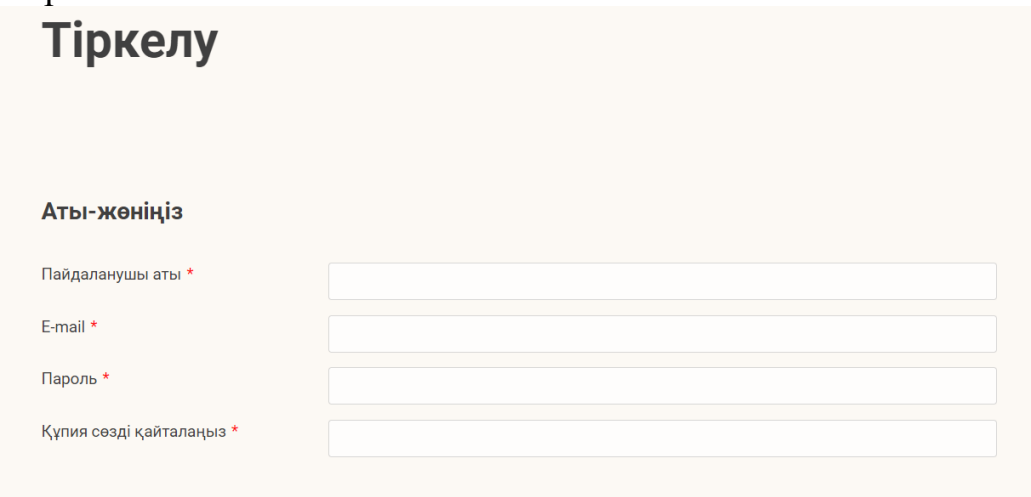


2.13 сурет. Профильді өзгерту формасы

Кейбір сайттарға тіркеусіз кіру мүмкін емес. Пайдаланушыға ыңғайлы болу үшін аккаунт жасалады, есептік жазбаның арқасында әлеуметтік желілерге кіре мүмкіндігі пайда болады.

Сайтқа тіркелу үшін (2.14 сурет) пайдаланушыдан қажет болатын ақпараттар:

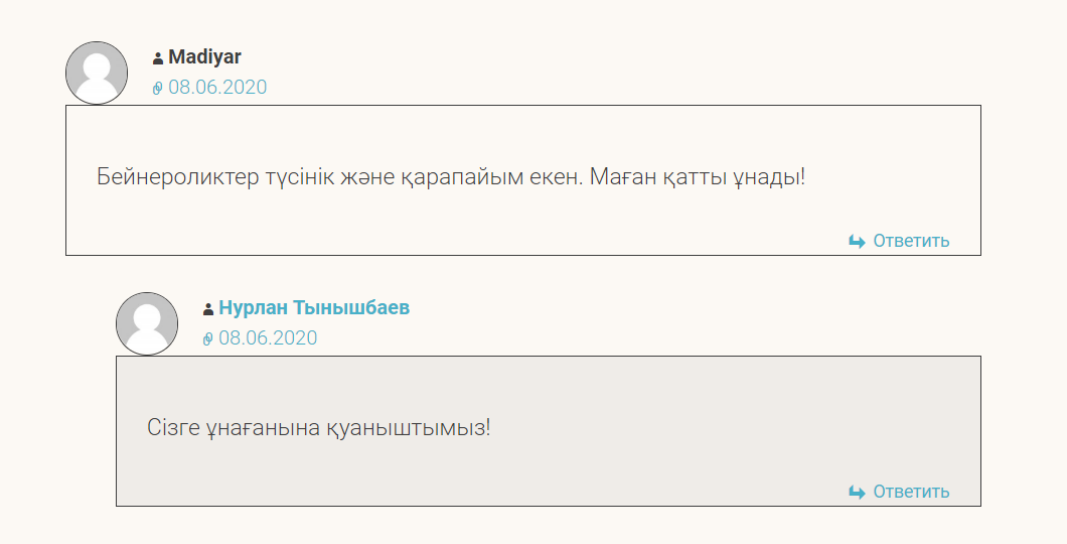
- аты-жөні,
- электрондық поштасы (e-mail),
- паролі.



2.14 сурет – Тіркелу формасы

Сонымен қатар, тіркелген қатысушы сайттың барлық беттеріне толық қол жеткізе алады. Оның қолынан:

- форумдарға қатысу
- жаңа тақырыптар құру
- сұрақ қою,
- мәлімдемелерге түсініктеме беру
- басқа пайдаланушының есеп жазбасын қарау
- қызықты сайттан жаңалықтар мен басқа ақпараттарды алу келеді.



2.15 сурет – Пікір қалдыру

3 Бөлім. Практикалық бөлім

3.1 «Kemel-NT» мектеп оқушыларына арналған веб-сайтты құру

Kemel-NT веб-сайты (3.1 сурет) – ол мектеп оқушыларына арналған көп салалы білім беру бағдарламасы болып табылады. Бұл бағдарлама білім беру жүйесінің қазіргі заманғы озық технологиясымен жабдықталған.

Kemel-NT білім беру орталығына келушілерге мекеме:

- Ағылшын тілін
- Математикалық курстарын
- ҰБТ-ге дайындық
- Ой-өрісті дамытуға арналған курстарын
- Логопед курстарын
- Мектепке даярлық
- Ұзартылған күн тобы

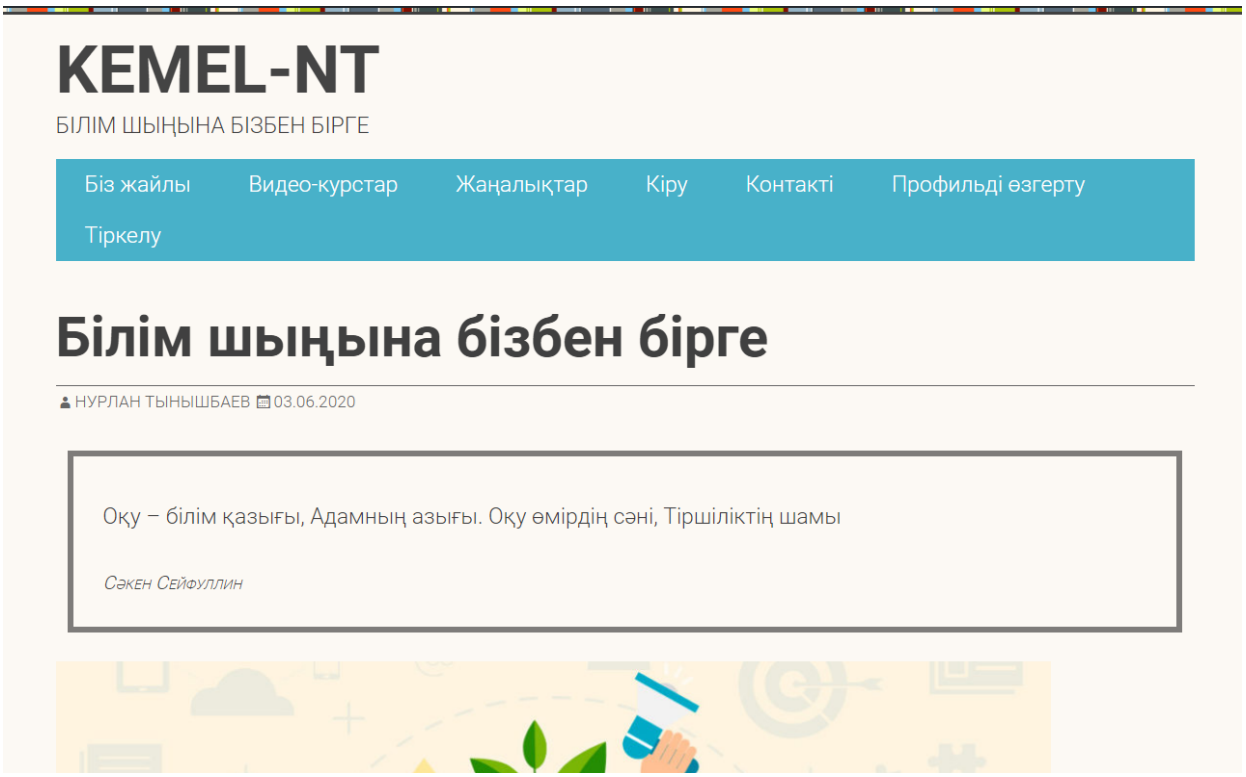
Оқушылар курсқа жазылар алдында деңгейді анықтайтын тестілеуден өтіп, топтарға бөлінеді. Мекемеде жалпы алғанда 11 кәсіби оқытушы жұмыс жасайды. Бұл мекеме жылдар бойы өзінің бәсекелестерінен қалыспай келуде. Қазіргі таңда Алматы қаласы бойынша түрлі жарыстарға қатысып, білім және сапа бойынша жүлделі орындар иелерінің бірі болып танылады.

Білім беру жүйесі білім беру орталығында және онлайн түрде өткізіледі. «Kemel-NT» веб-сайтында оқушылар бейнажазбаларды көре алады және өз пікірін немесе сұрақтарын түсініктеме ретінде бейнежазбаның астына қалдырып кете алады. Сайтта оқушыларға арналған форум ұйымдастырылған және мұнда оқушылар өз ойларын талқыға салып немесе білмеген заттарын сұрай алады. Сондай-ақ оқушылар алда болатын сабақтарын веб-сайтта «Сабақтар кестесін» арқылы көре алады.

Барлық идеялар мен ойларды жүзеге асыру үшін CMS мазмұнды басқару технологиясының WordPress платформасы қолданылды.

Веб-сайттың басқаларға қарағанда ерекшелігі:

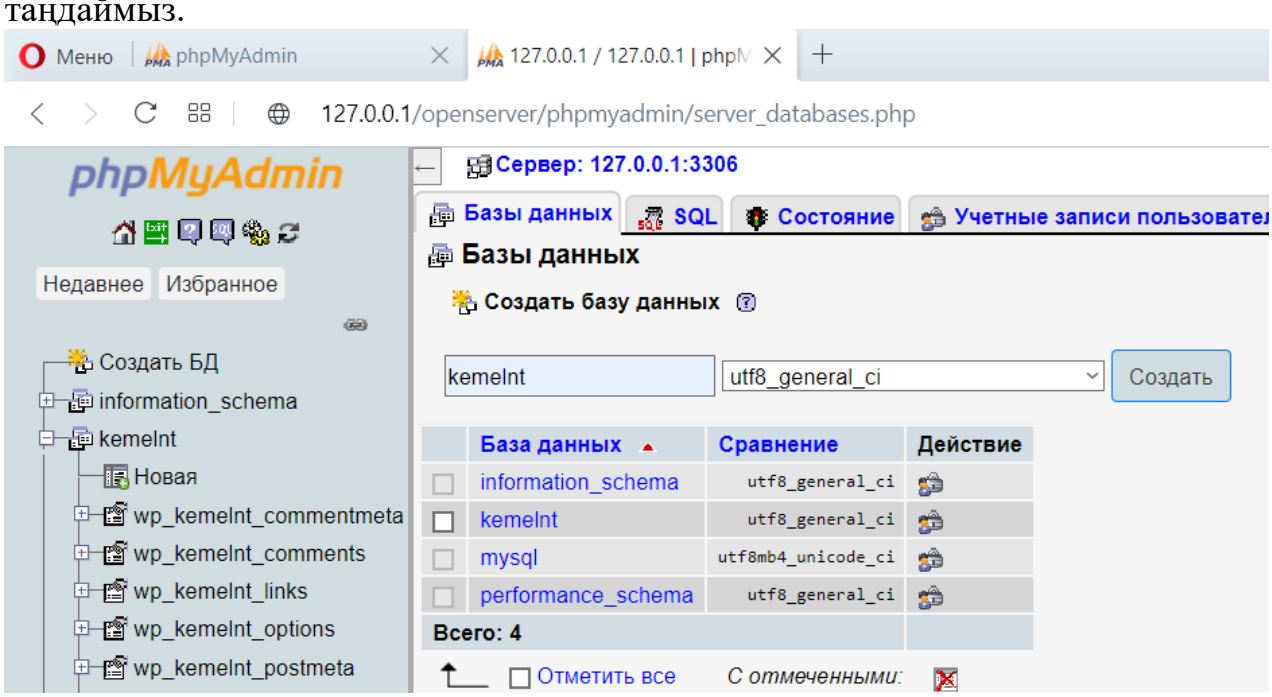
- Сайттың дизайны қарапайым, оқуға оңай;
- Веб-парақшалар ашық түсті болып келеді және бір қарағаннан-ақ тартымды көрінеді;
- Веб-сайт мекеменің өзіндік эмблемасын қолданады;
- Оқушылар форумдарда пікір-талас ұйымдастыра алады;
- Бейне-жазбаларды онлайн түрде көреді;
- Сабақ кестелерін қарай алады;
- Веб-сайт сенімді қорғаныспен жабдықталған.



3.1 сурет – «Kemel-NT» веб-сайтының басты беті

3.2 Веб-сайттың жұмысы мен интерфейсін әзірлеу

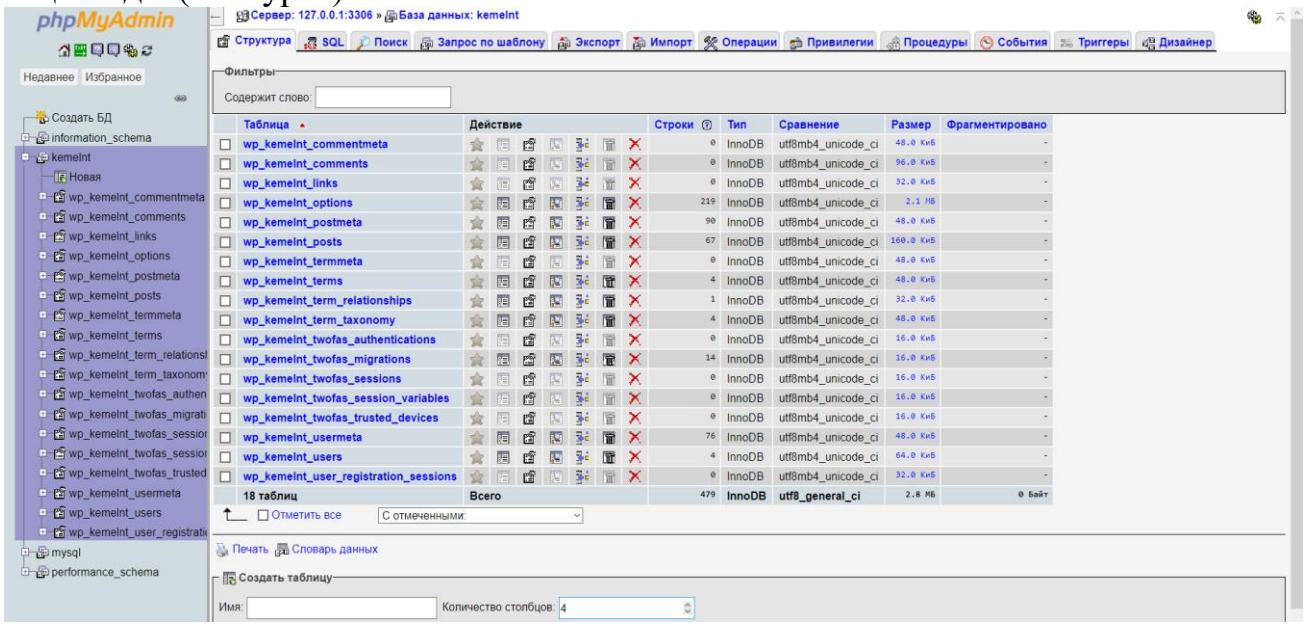
Жұмыс барысы веб-сайтқа дерекқорларды құрумен басталады. 3.2 суретте көрсетілгендей алғашында веб-сайттың атын, содан соң «utf8_general_ci» таңбаларды салыстыруға, сұрыптауға арналған кодтау түрін таңдаймыз.



3.2 сурет – Дерекқорлар базасын құру

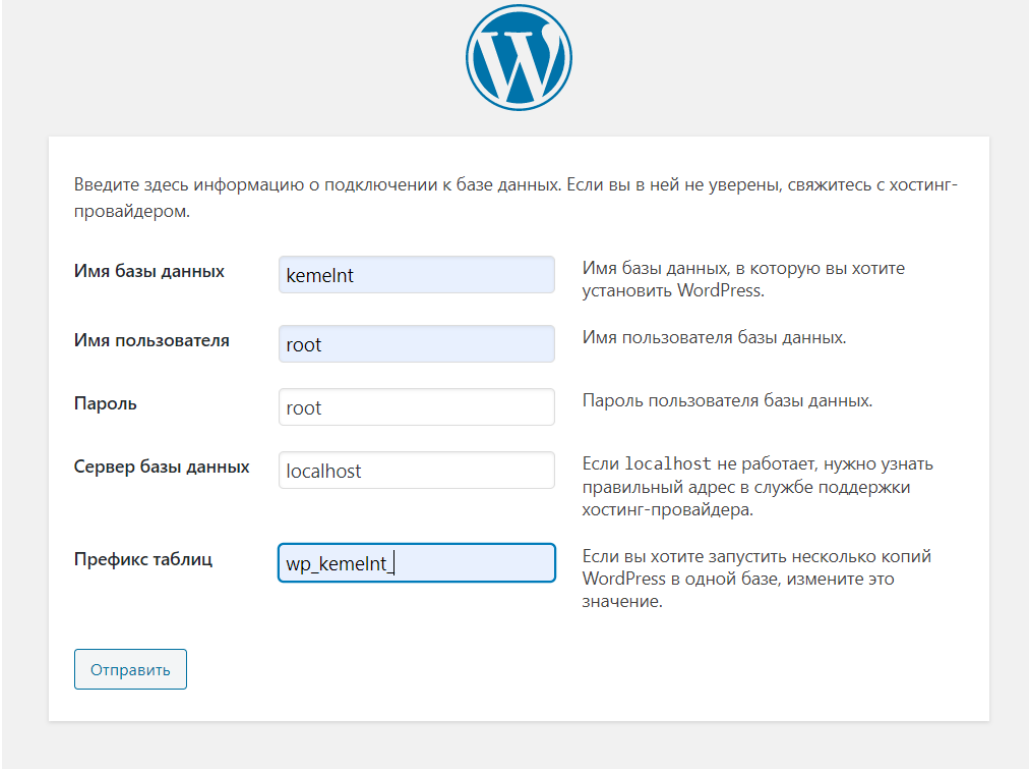
Веб-сайт жайлы мәліметті Open Server Panel программасының «domains» бумасына көшіріп, phpMyAdmin жүйесін қайта жүктейміз.

Жүктегеннен кейін «kemelnt» дерекқорлар базасында кестелер тізбегі сақталады (3.3 сурет).



3.3 сурет – Кестелер тізбегі

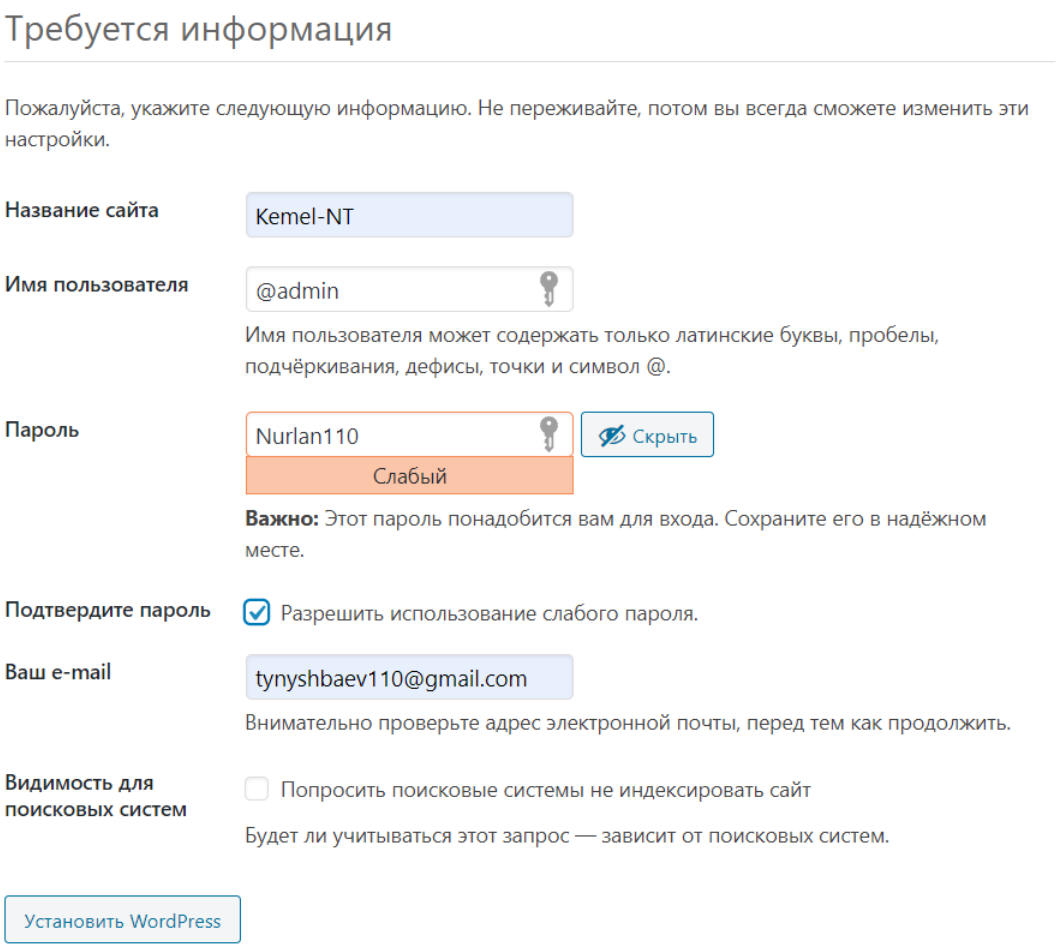
Дерекқор базасында кестелер тізбегін құрып болғаннан кейін WordPress платформасын дерекқормен байланыстырамыз (3.4 сурет). Мұнда дерекқорлар базасының атын, қолданушының аты мен паролын, дерекқордың серверін және кесте атауын береміз.



3.4 сурет – Веб-сайтты дерекқор базасымен байланыстыру

Дерекқор платформамен сәтті байланысқаннан кейін веб-сайт WordPress-ке тіркелінеді (3.5 сурет). Тіркелу барысында веб-сайттың атауын,

қолданушының атын (әкімшінің), парольін, электронды поштасын енгізіп веб-сайтты орнатамыз.

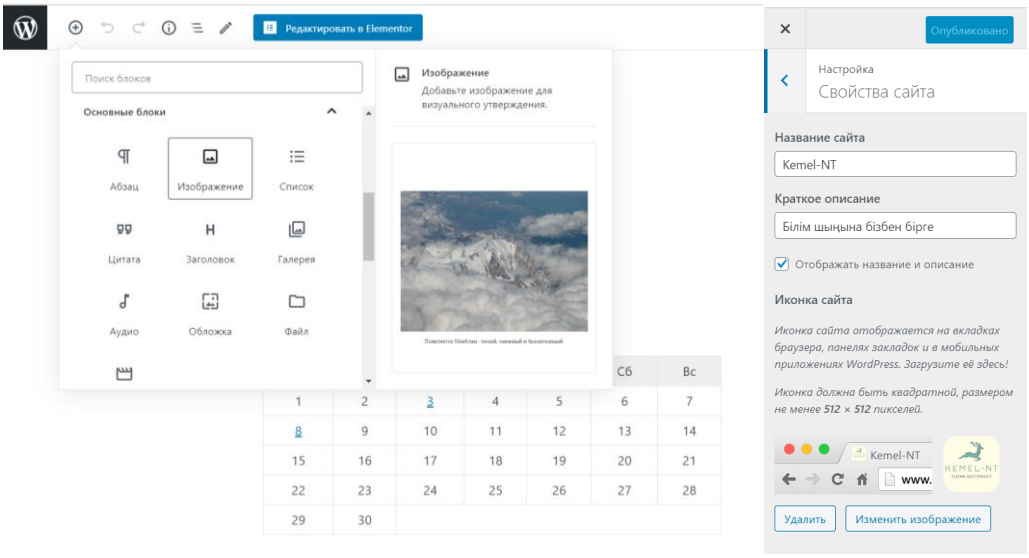


3.5 сурет – Веб-сайтты WordPress-ке тіркеу және орнату

WordPress платформасына сәтті тіркелгеннен кейін керекті өрнектермен тақырыпты таңдап сайттың дизайнына көшеміз.

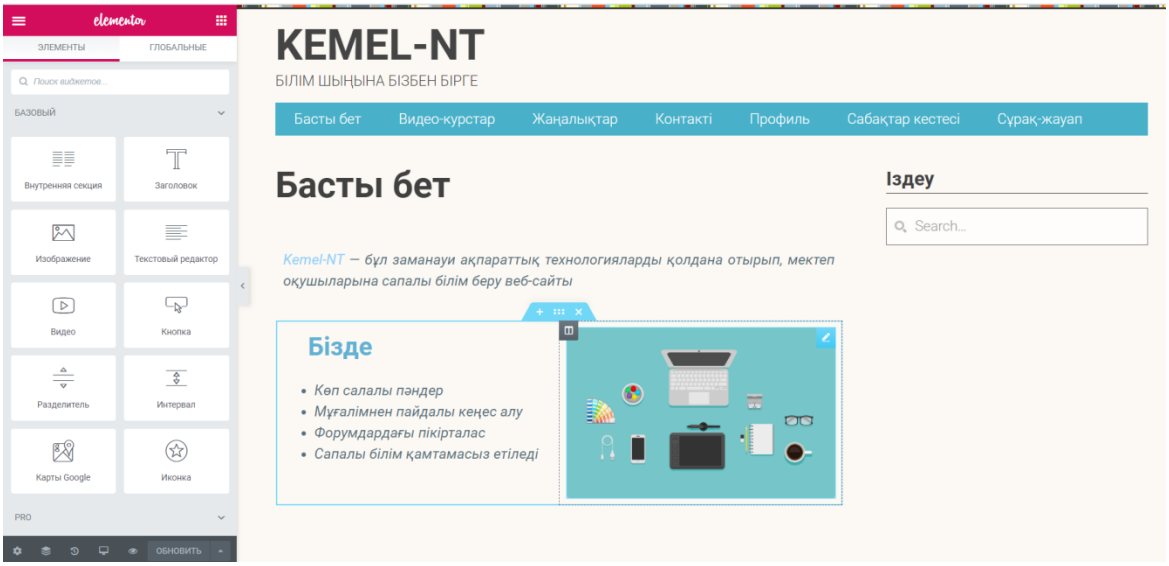
Веб-парақшаларды құрастыру, мәліметтерді еңгізу, жою, өңдеу және т. б. іс-әрекеттерге WordPress-тің кірістірілген редакторы мен Elementor плагинінің көмегімен жүзеге асырылды.

WordPress платформасының кірістірілген редакторлары веб-парақшаларға «блок» құралын қолдану арқылы мәтіндерді, суреттерді, бейне жазбаларды енгізу үшін және веб-сайттың қасиеттерін өзгертуге үшін қолданылды.



3.6 сурет – WordPress-тің кірістірілген редакторы

Elementor (3.7 сурет) – бұл заманауи визуалды конструктор. Оны кез келген WordPress тақырыбына пайдалануға болады. Elementor WordPress-тің бос парақшасына да орнатуға болады. Оны орнатқаннан кейін сіз алдын-ала теңшелген виджет модульдерін қолданып кез-келген бетті өз қалауыңызша өңдей аласыз.

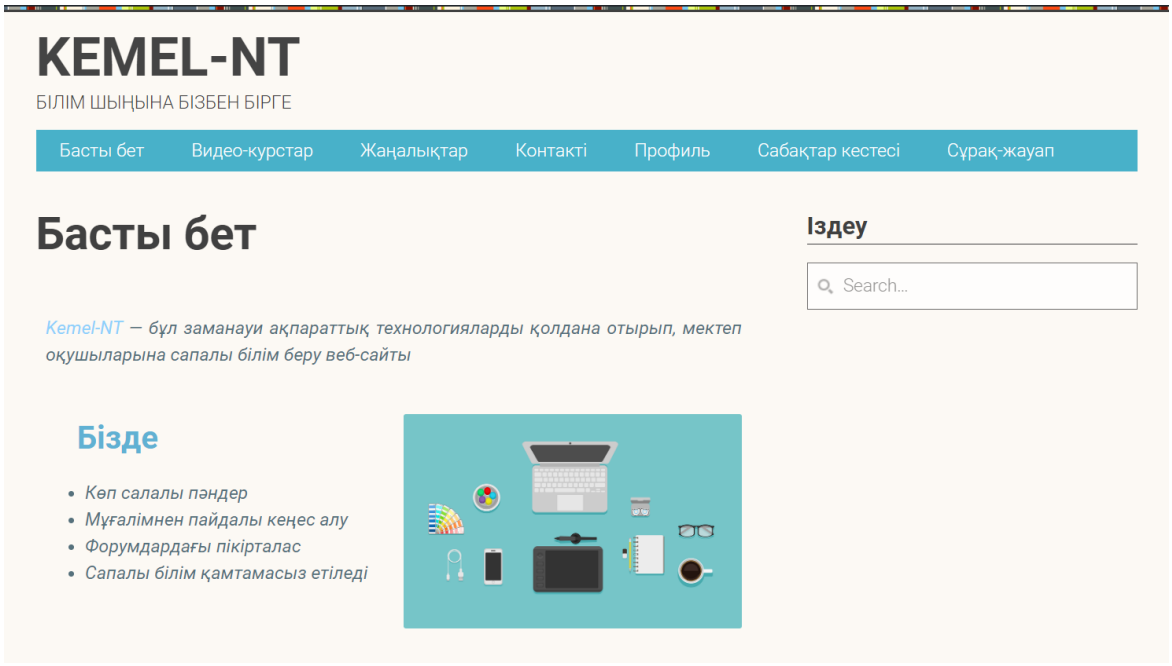


3.7 сурет - Elementor плагині

Келесі кезекте әзірленген веб-сайтқа шолу жасайық. Мұнда пайдаланушы үшін:

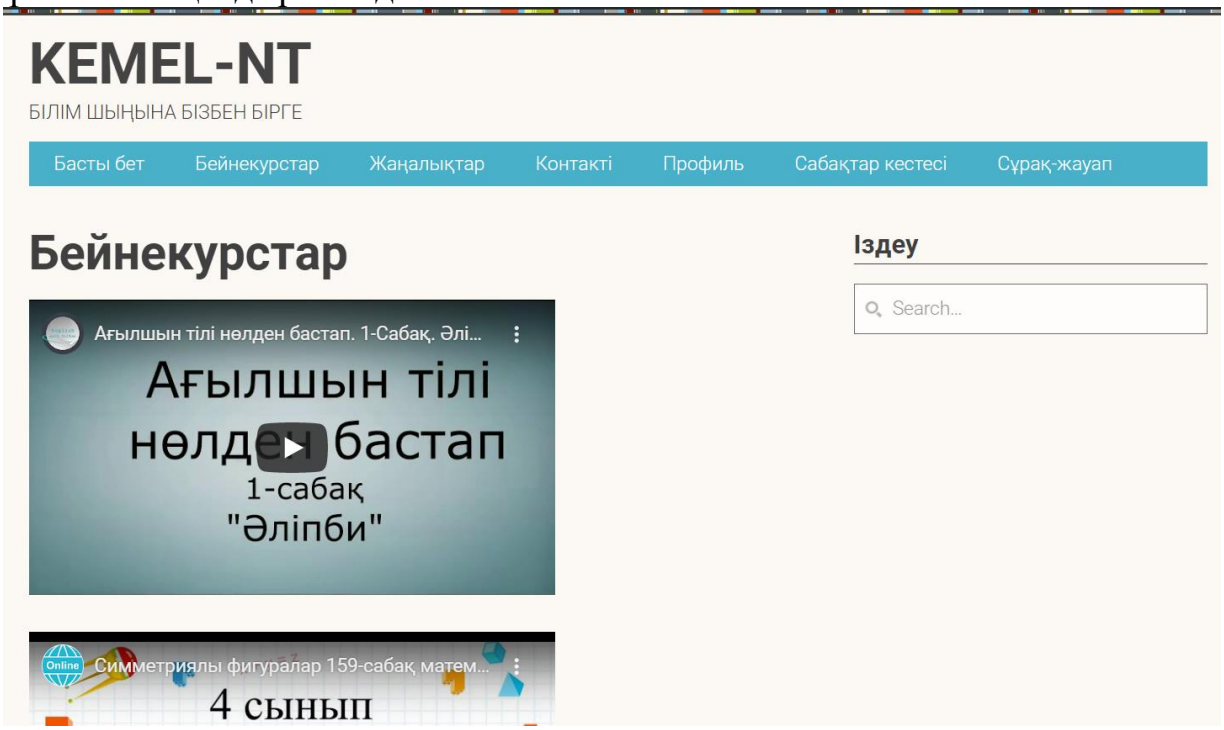
- Басты бет;
- Бейнекурстар:
- Жаңалықтар;
- Контакті;
- Профиль;
- Сабақтар кестесі;
- Сұрақ жауап қойындысы ұсынылады.

Басты бетте (3.8 сурет) – «Kemel-NT» білім беру орталығы жайлы ақпараттар болады. Мұнда оқушылар өткізілетін сабақтар жайлы ақпаратты біле алады.



3.8 сурет – Веб-сайттың Басты беті

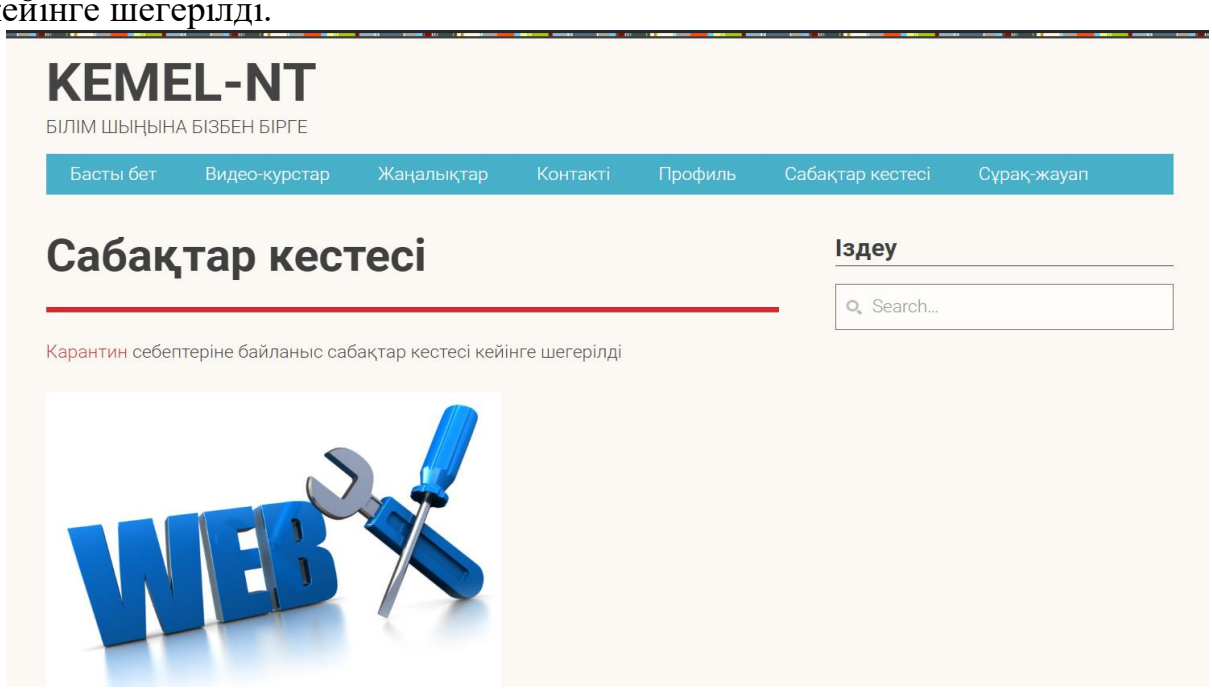
«Бейнекурстар» парақшасында (3.9 сурет) оқушылар өзінің таңдаған пәндерінің бейнежазбаларын онлайн түрде көре алады. Егер оқушы түсінбеген, не сұрақтары бар болған жағдайда бейнежазбанын астына түсініктеме қалдыра алады.



3.9 сурет – «Бейнекурстар» парақшасы

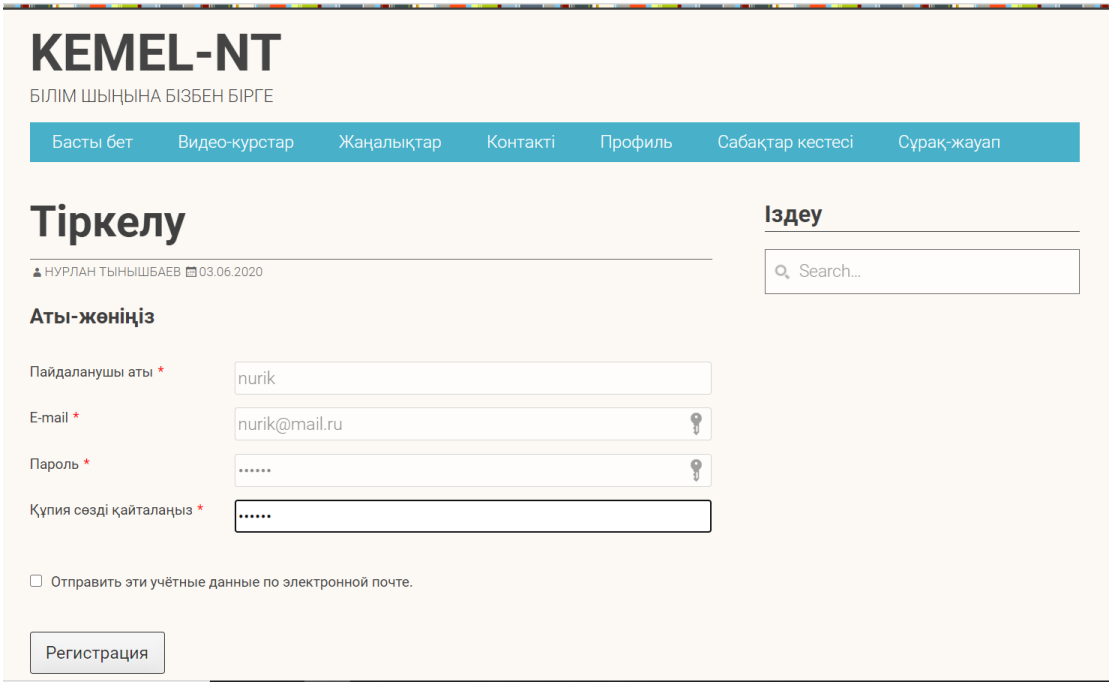
«Сабақтар кестесі» веб-парақшасында (3.10 сурет) оқушылар алда болатын сабақтарының күні мен уақытын көре алады.

Қазіріг таңда карантин себептеріне байланысты сабақтар кестесі кейінге шегерілді.



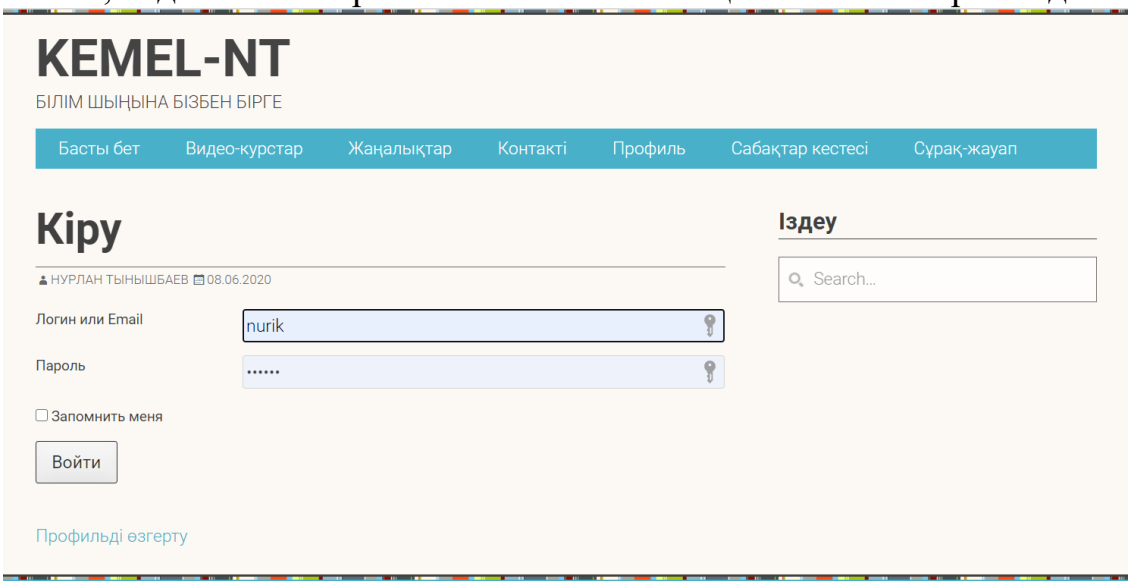
3.10 сурет – «Сабақтар кестесі» парақшасы

Келесі парақшада оқушылар өздерін тіркеп (3.11 сурет) кейін «Кіру» батырмасын басып веб-сайтқа кіреді. Егер оқушы өзінің есеп-жазбасын өзгерткісі келген жағдайда «Профильді өзгерту» парақшасында жүзеге асыра алады.



3.11 сурет - Жаңа пайдаланушыны тіркеу

3.12 суретте тіркелген пайдаланушыны веб-сайтқа кіру формасы көрсетілген. Мұнда оқушы өзінің қолданушы атын немесе электронды поштасын, содан кейін паролын жазып веб-сайтқа өз атынан кіре алады.

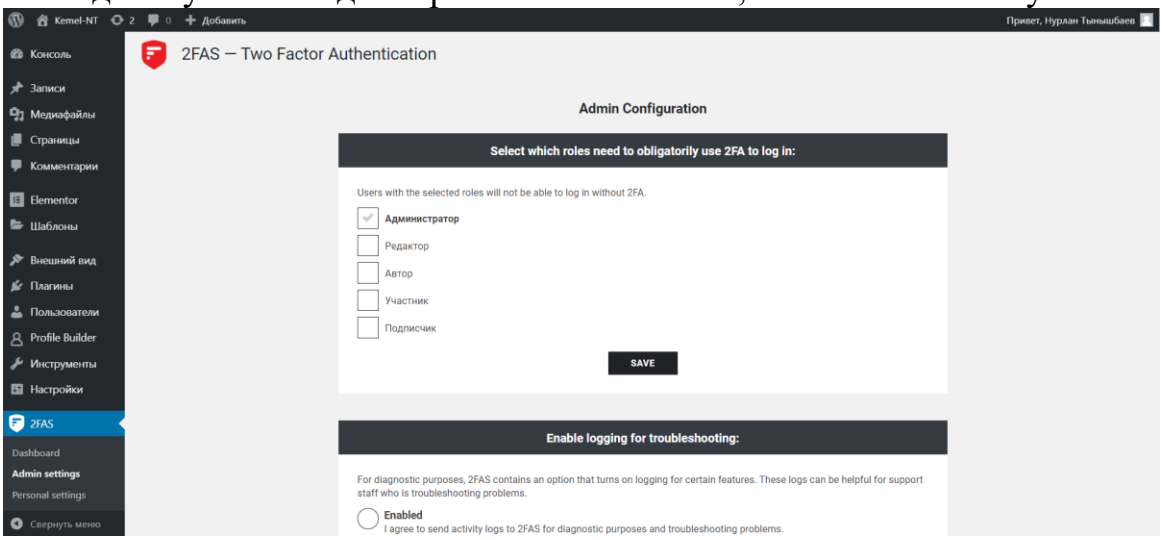


3.12 сурет – Веб-сайтқа кіру

3.3 Веб-сайтқа қорғаныс ұйымдастыру

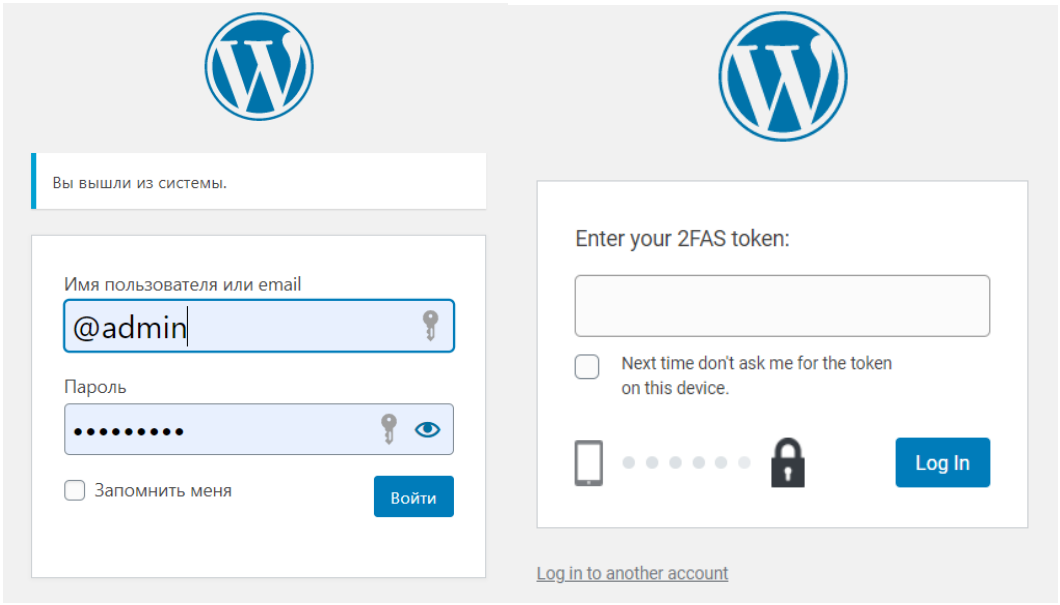
Екі факторлы аутентификация – бұл екі түрлі аутентификациялық деректерді сұрау арқылы қандай да бір сервисте (әдетте Веб-сайттарда) пайдаланушыны сәйкестендіру әдісі. Ол екі қабатты қорғау жүйесі болғандықтан, есептік жазбаға рұқсатсыз кіруден тиімдірек қорғауды қамтамасыз етеді. Іс жүзінде бұл: бірінші кезекте - пайдаланушы аты мен паролын, екінші кезекте – смс, электрондық пошта немесе бағдарламалық жасақтама құралы арқылы келетін арнайы код.

2FAS (3.13 сурет) – плагинінде хабарлама арнайы бағадарламалық жасақтама арқылы келеді. «Kemel-NT» веб-сайтында екі факторлы аутентификация тек әкімшіде ғана орнатылған. Себебі, веб-сайтта тек екі ғана пайдаланушы болады: біріншісі – ол әкімші, екіншісі – жазылушы.



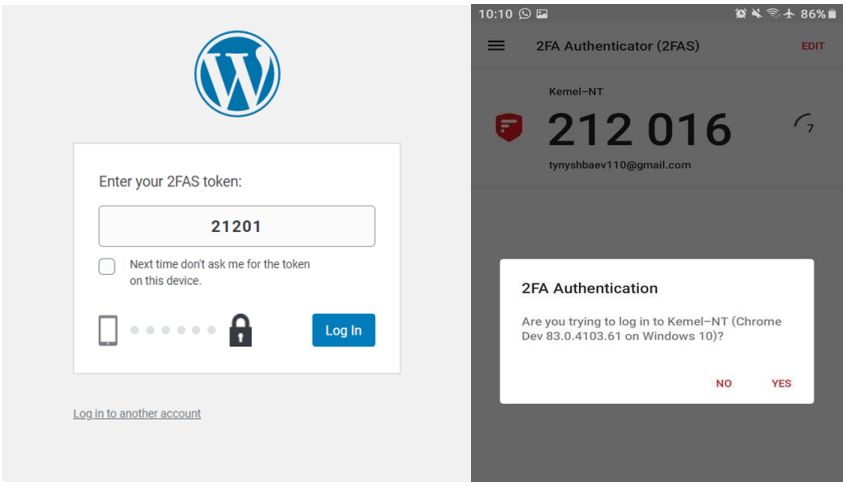
3.13 сурет – Екі факторлы аутентификация параметрі

2FAS – плагинінің іс-жүзінде тексеріп көрейік. Бірінші кезекті – әкімшінің атынан шығып одан кейн қайта кіріп көреміз. Әкімшінің аты мен паролын тергеннен кейін платформа кіру үшін 3.14 суретте көрсетілгендей 6 санды кодты сұрайды.



3.14 сурет – Қос факторлы аутентификация сұраудың көрінісі

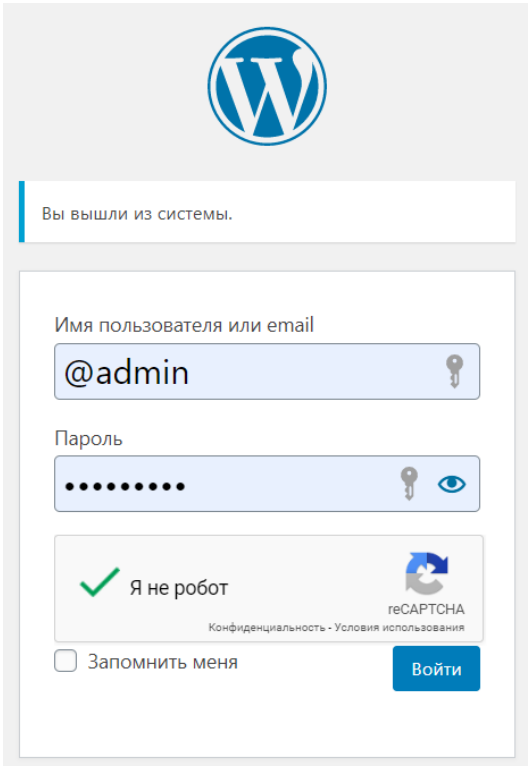
2FAS программасы 6 саннан тұратын кодты смартфонға арнайы орнатылған бағдарламаға жібереді. Келген кодты (3.15 сурет) «yes» батырмасы арқылы, не 6 санды кодты теру арқылы растай аламыз.



3.15 сурет – Смартфонға келіп түскен коды енгізу

reCAPTHCHA - бұл Карнеги Меллон Университетінде веб-сайттарды спам-боттардан қорғауға және сонымен бірге кітап мәтіндерін цифрландыруға көмектесетін жүйе.

reCAPTHCHA 3.16 суретте көрсетілгендей веб-сайтқа кірер алдында немесе тіркелер алдында іске қосылады.

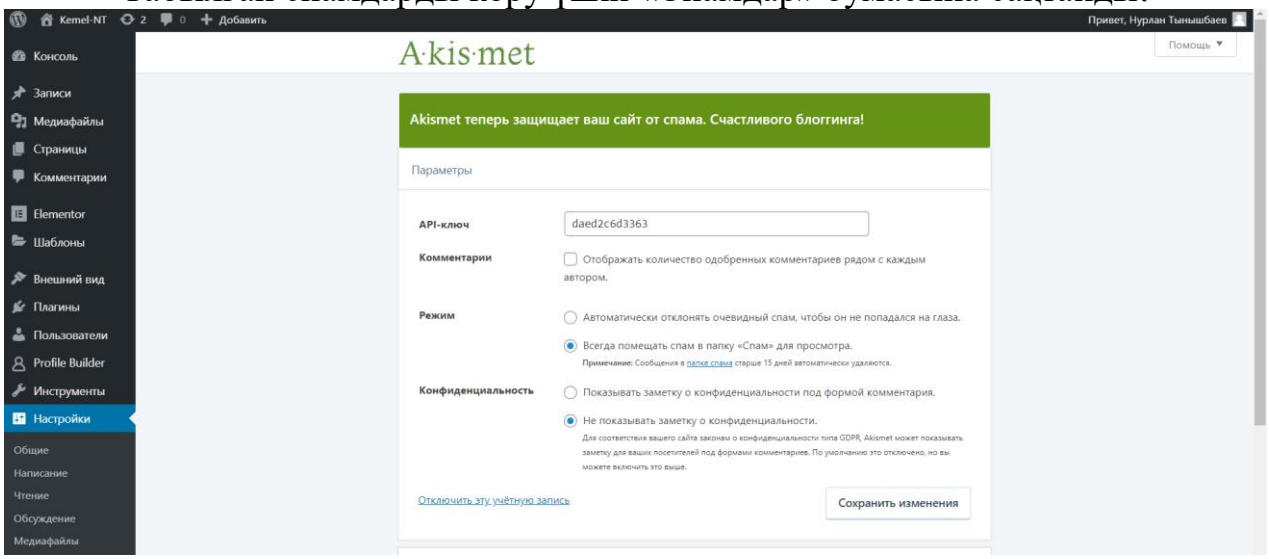


3.16 сурет – reCAPTHCA көмегімен спам-боттардан қорғану жүйесі

Akismet – веб-сайтты зиянды спамдардың жариялануына жол бермеу үшін программа жаһандық спам деректер базасы бойынша байланыс формасындағы пайдаланушылар қалдырған түсініктемелер мен мәліметтерді тексерістен өткізеді.

Aksimet (3.17 сурет) WordPress платформасына арнайы API-кілті арқылы орнатылады. Программа 2 түрлі режимде пікірлерді сұрыптай алады:

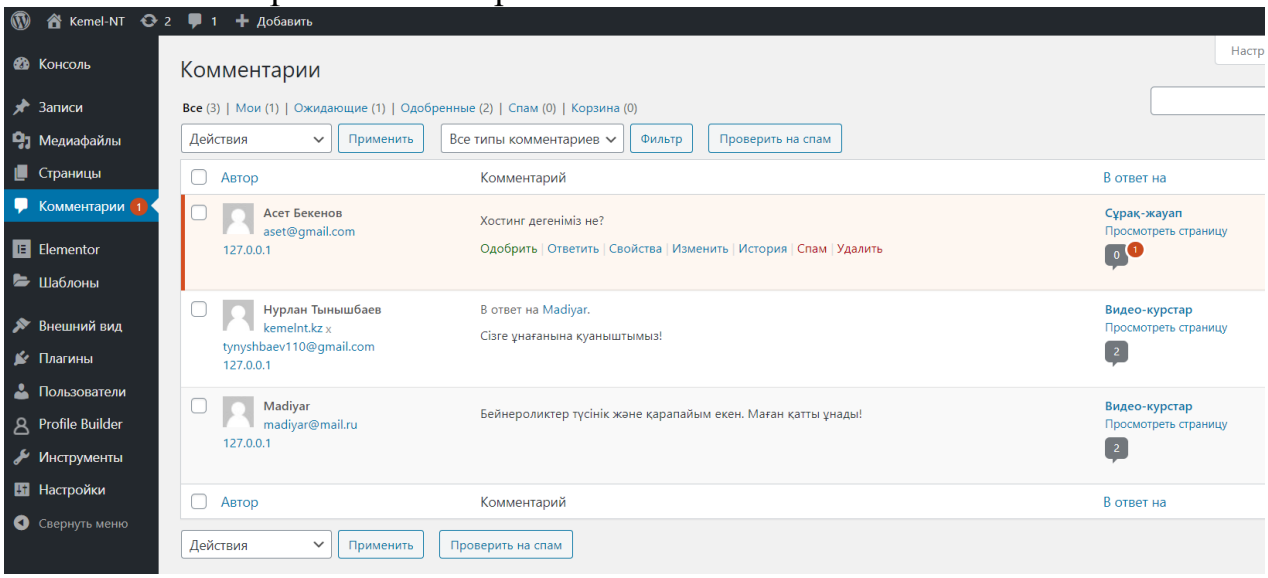
- Автоматты түрде спамдарды жою
- Табылған спамдарды көру үшін «Спамдар» бумасына сақтайды.



3.17 сурет – Akismet – спамдардан қорғауға арналған плагин

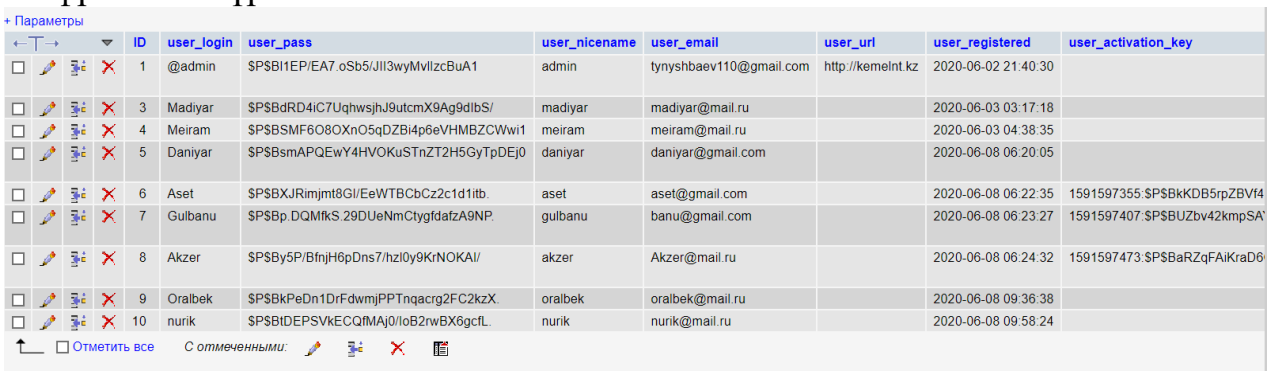
Веб-сайтқа пайдаланушы қалдырған түсініктемені 3.18 суретте көрсетілгендей модерациялаудан өткізе аламыз. Келіп түскен түсініктемені әкімші:

- Қабылдауға;
- Жауап беруге;
- Қасиеттерін қарауға;
- Өзгертуге;
- Жіберген пайдаланушыны көруге;
- Спамға жіберуге;
- Жоюға мүмкіншілігі бар.



3.18 сурет – Түсініктемелерді модерациялаудан өткізу

MD5 – хэш функциясы арқылы жүзеге асатын шифрлеудің түрі, яғни байттардың үлкен және ұзын тізбегін 128 битке айналдыратын хэштеу алгоритмі. phpMyAdmin келіп түскен пайдаланушылар парольдерінің шифрланған түрі.



3.19 сурет – MD5 хэштеу алгоритмі

4 Ақпараттық қауіпсіздік тәуекелдері

4.1 Тәуекелдерді бағалау және анализ

Дипломдық жобаның Ақпараттық қауіпсіздік тәуеледері бөлімінде веб-сайтта пайда болатын тәуекелдерді есептейміз.

Тәкелеге бағалау беру кезінде активтердің құндылығын, қауіптерін және осалдықтарын анықтаймыз. Анықтау шаралары жүргізігеннен кейін ықтималдық салдарын анықтап, оған қорғану әдістерін жүргіземіз.

Екі тәуекел бойынша бағалау әдісі – қауіптің туындау ықтималдылығын бағалаудан және зақымдану ықтималдылығын бағалаудан тұрады. Келтірілетін әдістеме бойынша тәуекел келесі формуламен анықталады: тәуекел=: ықтималдылық * зақым.

Екі тәуекел бойынша бағалау әдісі үш негізгі кезеңнен тұрады:

1. Тәуекелдердің бастапқы есебі. Мұнда анықталған тәуекелдерге есептеу жүргізіліп, тәуекелдің қолайлы, не қолайсыз екенін талдаймыз. Қолайсыз тәуекелдер бар болған жайғдайда оларды екінші кезең негізінде қарастырамыз.

2. Қолайсыз тәуекелдерге арналған шараларды анықтау. Егер кейбір тәуекелдер қолайлы тәуекелдердің бастапқы немесе оратша деңгейінен асып қолайсыз тәуекелдер деңгейіне жеткен жағдайда үш параметр бойынша есептеу жүргізіп үшінші кезеңге жіберіледі.

3. Қайта есептеу. Бұл кезеңде жоғарғы деңгейлі тәуекелдер үш параметр бойынша қайта есептелінінеді. Тәуекелдің деңгейіне қарай есептеуден кейін бір немесе екі сатыға түседі.

Тәуекелдердің қауіптер туындату шкаласы мен шығын көлемінің шкаласы ISO-27005 стандартының [1] Е қосымшасы бойнша жүргізілді. Тәуекелдерге талдау барысында активтерді ықтимал салдарының құпиялылығына, тұтастықтығына және осалдылықтарына қарай бағаланды.

Тәуекелді есептеу қауіптердің туындау ықтималдылығы мен шығын көлемінің шкаласы арқылы басталады. Қауіптердің туындау ықтитмалдылығы мен шығын көлемінің шкаласы 4.1 және 4.2 кестеде көрсетілген.

4.1 кесте – Қауіптердің туындау ықтималдылық шкаласы

Қауіптердің туындау ықтималдылық шкаласы	
Ықтималдылық деңгейі	Қауіптің туындау ықтималдығы
0 - өте төмен	5 жылда шамамен 2-3
1 - төмен	3 жылда шамамен бірнеше рет және сирек
2 - орташа	Жылына шамамен бірнеше рет
3 - жоғары	Айына шамамен 1 рет
4 – өте жоғары	Айына шамамен бірнеше рет

4.2 кесте – Шығын көлемінің шкаласы

Шығын көлемінің шкаласы	
Деңгейі	Ақшалай сипаттамасы
0 - өте төмен	50 000 теңгеге дейін
1 - төмен	100 000 теңгеге дейін
2 - орташа	300 000 теңгеге дейін
3 - жоғары	500 000 теңгеге дейін
4 - өте жоғары	1 000 000 теңгеден жоғары

Тәуекелдердің қолайлылық шкаласы 4.3 кестеде көрсетілген.

4.3 кесте - Тәуекелдердің қолайлылық шкаласы

Тәуекелдердің қолайлылық шкаласы		
Деңгейі	Жоғалту	Сипаттамасы
0-ден 2-ге дейін	100 000 тг дейін	Қолайлы тәуекел
3-тен 5-ке дейін	300 000 тг дейін	Орташа-қолайлы тәуекел
6-дан 8-ге дейін	500 000 тг жоғары	Қолайсыз тәуекел

Ақпаратты өңдеу құралдарын, әдістерін және қорғалатын ақпарат тізбесін талдау нәтижесінде активтердің келесі тізбесімен бөліп көрсетуге болады:

- Дерекқорлар базасы;
- Windows Server 2012 Standard;
- WordPress платформасы;
- Желілік жабдықтар;
- Сервер;

4.4 кесте– Тәуекелдерді бағалаудың қорытынды кестесі

№	Қауіптер	Осалдық	Ең жоғарғы деңгей	Тәуекелді жою шаралары	Тәуекелдің қалдық деңгейі
1 Дерекқорлар базасы					
1.1	Рұқсатсыз кіру	Қолжетімділікті бақылаудың жеткіліксіздігі	3	Қолжетімділікті шектеу, парольдік қорғау	2
1.2	Деректерді бұрмалау	Тексеру мен жаңартулардың уақылы жүргізілінбеуі	8	Деректерді қалпына келтіру жүйелері	3
1.3	Деректерді ұрлау	Техникалық тарату арналары арқылы ағу	2	Радиожиілікті жоққа шығаратын құрылғылар	1
2 Windows Server 2012 Standard					
2.1	Зиянды бағдарламаны енгізу	Үнемі тексерулер мен жаңартулардың болмауы, антивирустық қорғаныстың болмауы	5	Касперский антивирустық бағдарламалық жасақтамасы	3
2.2	Құпия сөзді автоматты таңдау үдерісі.	Сұраныстарды өңдеу үдерісінде уақыт бойынша шектеудің болмауы	3	Сұрауларды өңдеу кезінде құпия сөзді шифрлау және уақытқа шектеу қою	1
2.3	Модификациялау	Windows Server бумасына	3	Бумаларды қорғауға арналған	0

		қорғаныстың болмауы		программа	
3 WordPress платформасы					
3.1	Спам-боттардың пайда болуы	Спам-боттардан қорғанатын тиісті плагиндердің болмауы	5	Aksimet спамдардар қорғау программасы	2
3.2	Брутфорстік шабуыл	Веб-сайт баяу жұмыс істейді	4	Платформаға файервол орнату	2
3.3	Sql инъекциясы	Қорғаныс шараларының ұйымдастырылмауы	3	PHP бағдарламау тілінде жазылған арнайы кодты енгізу	1
4 Желілік жабдықтар					
4.1	Жұмыстағы іркіліс	Физикалық қатынаудан сенімді қорғанудың болмауы, сенімсіз парольдер, желіні дұрыс конфигурацияламау	5	Іркілісті тудыратын құрал-жабдықтарды жаңарту	3
4.2	Трафикті ұстап қалу	Рұқсатысыз кіруден сенімді қорғаныстың болмауы, сенімсіз	5	Желіні сканерлеуге арналған Angry IP Scanner	3

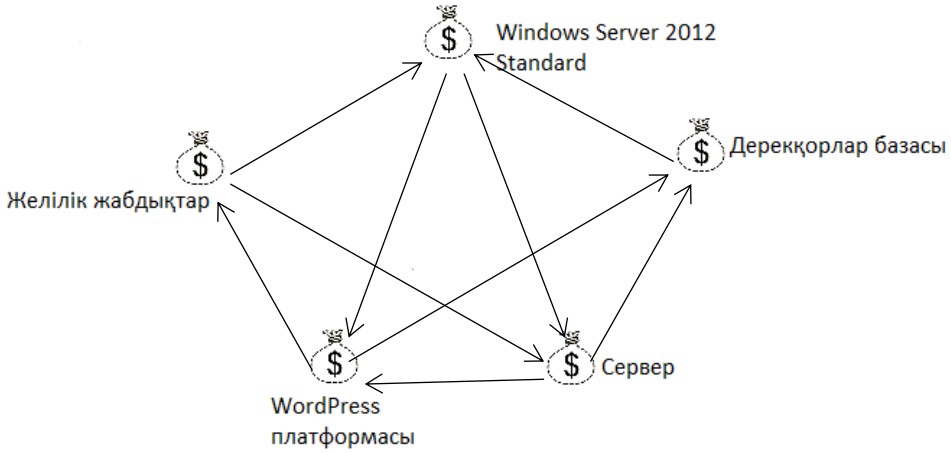
		парольдер		программасы	
4.3	Деректерді ұстап алу	IP-мекенжайының көздерін және ресурстарын ауыстыру.	3	Трафикті сүзгіден өткізу	1
5 Сервер					
5.1	Жұмыстағы іркіліс	Сервер жағдайын бақылау жүйесінің болмауы	7	IDS / IPS жүйесі	4
5.2	Рұқсатсыз кіру	Қолжетімділікті бақылаудың жеткіліксіздігі	5	Қолжетімділікті шектеу, парольдік қорғау	3
5.3	Басқаруды ұстап қалу	Сенімді қорғаудың, қолжетімділікті шектеудің, тұрақты тексерулердің және жаңартудың болмауы	6	Қолжетімділікті шектеу, парольдік қорғау	4

4.2 CORAS құралымен тәуекелдерді талдау

Coras – қауіпсіздік тәуекелдерін талдауға арналған әдіснама болып табылады. Бұл әдіснама тәуекелдер мен қатерлерді модельдеу үшін қолданылады.

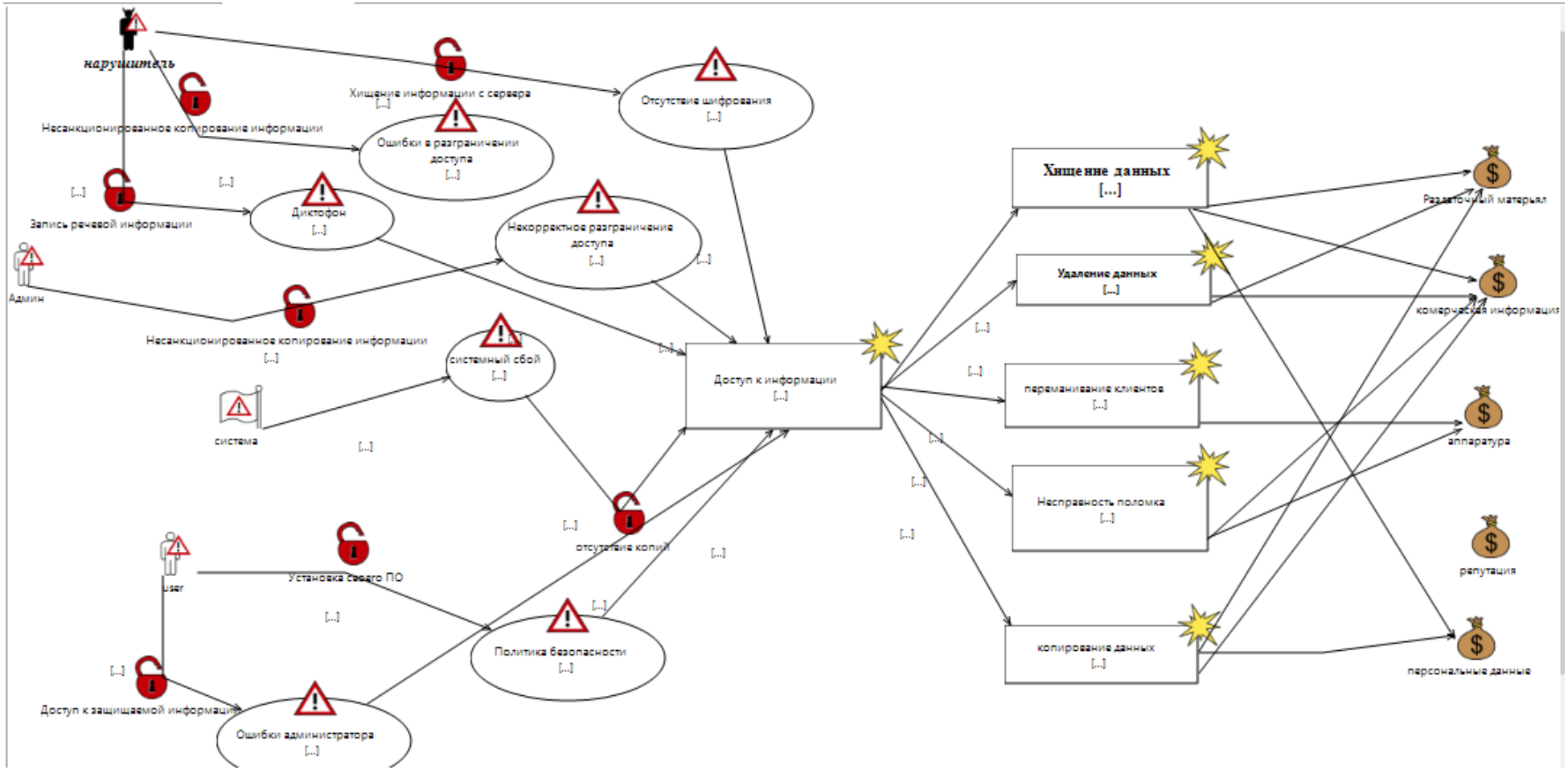
Программа методологиясы Information Society Technologies бағдарламасы аясында әзірленген және ол EventTreeAnalysis, HazOp сынды тәуекелдерге талдау жүргізу, оны нақтылау жәнеде біріктіру әдістерінен тұрады [2]. Coras обьектілі модельдеуді қамтамасыз үшін UML-графикалық сипаттау тілін қолданады. UML-графикалық сипаттау тілі бағдарламаны анықтау, жобалау және т.б мақсаттарда жұмыс жасайды.

Дипломдық жобада ақпараттық қауіпсіздіктің тәуекелдерін талдау жұмысында активтерді қолданып және оның диаграммасын салдық. Активтер 4.1 суретте бейнеленген.



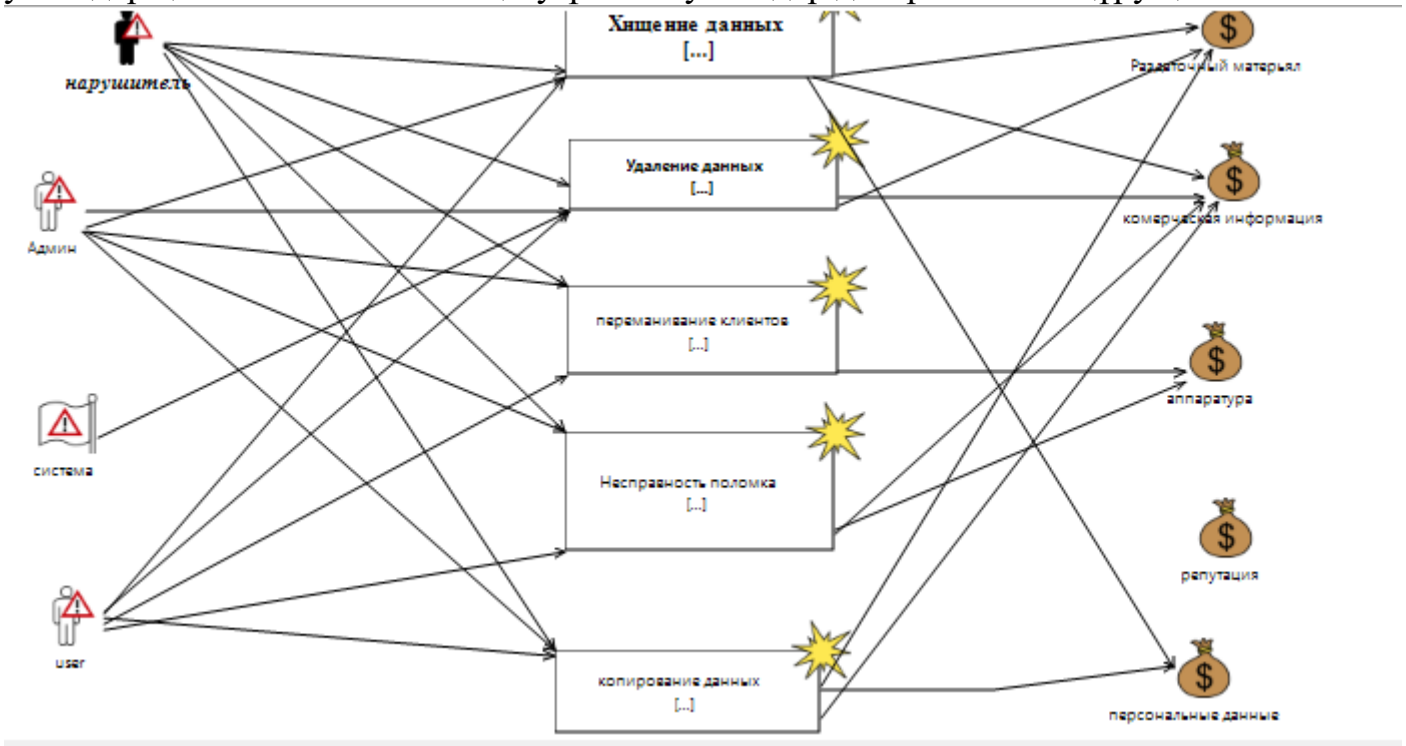
4.1 сурет – Активтер диаграммасы

4.1 кестедегі активтерді пайдалану арқылы жағымсыз инцидент сценарийін жүзеге асыру ықтималдығын келтіреміз. Нәтижесінде 4.2 суретте көрсетілген қауіптер моделін аламыз. Басында табылған осалдылықтарды өз пайдасында қолданатын зиянкестер қауіп-қатерді іске асырады. Салдарынан активтердің осалдылығын, оның себебі мен жою көздері жайлы мағұлмат аламыз. Мысалы, зиянкес арнайы скрипт бойынша жұмыс істейтін спам-боттарды қолданып қауіпті сұрауларды жіберу арқылы веб-сайттың пайдаланушыларына қауіп-қатер төндіреді.



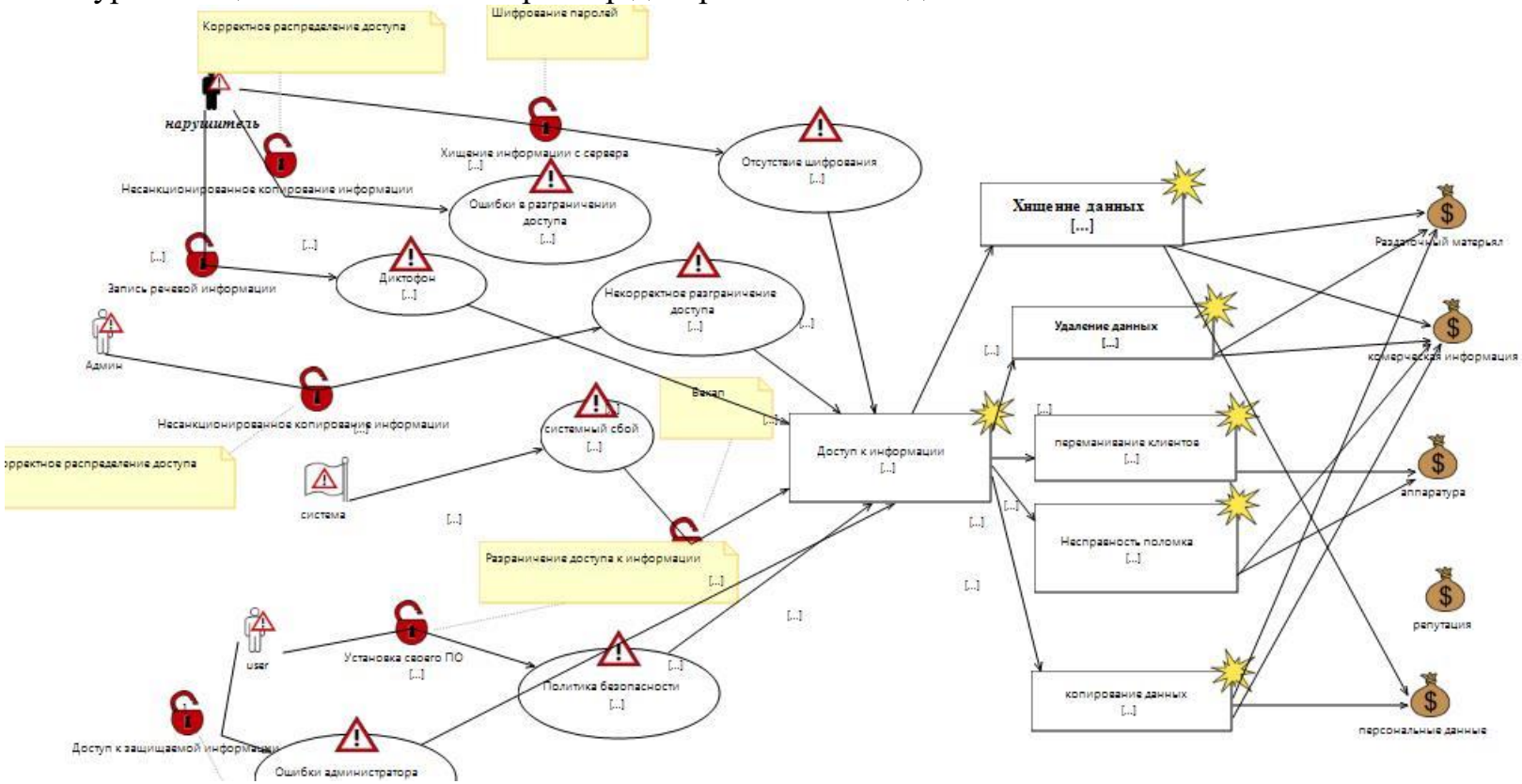
4.2 сурет – Қауіптер диаграммасының моделі

Қандай тәуекелдер қолайсыз екенін анықтау үшін тәуекелдер диаграммасын құру қажет.



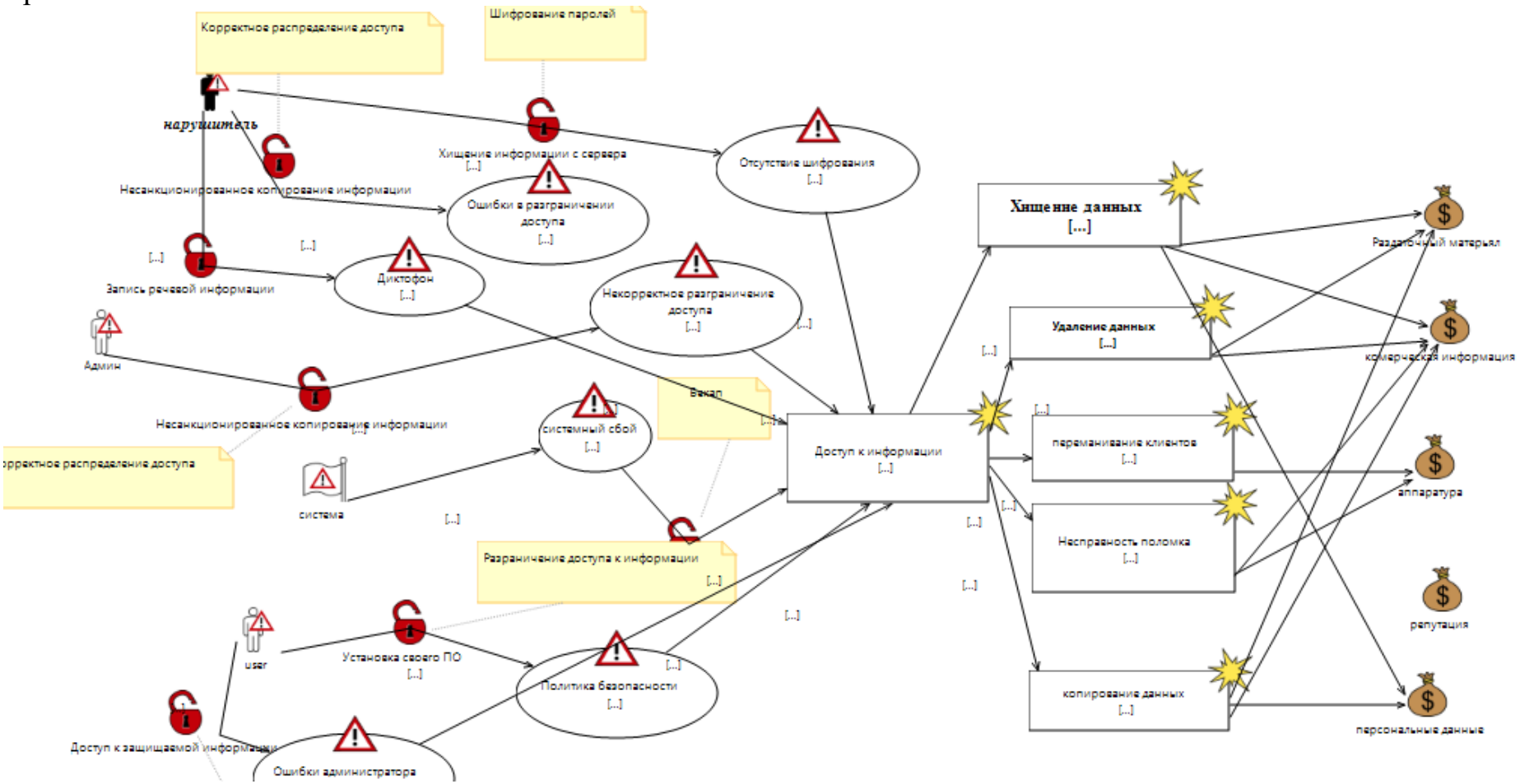
4.3 сурет – Тәуекелдер диаграммасы

Келесі суретте ықтимал сипаттамалары бар диаграмма салынады.



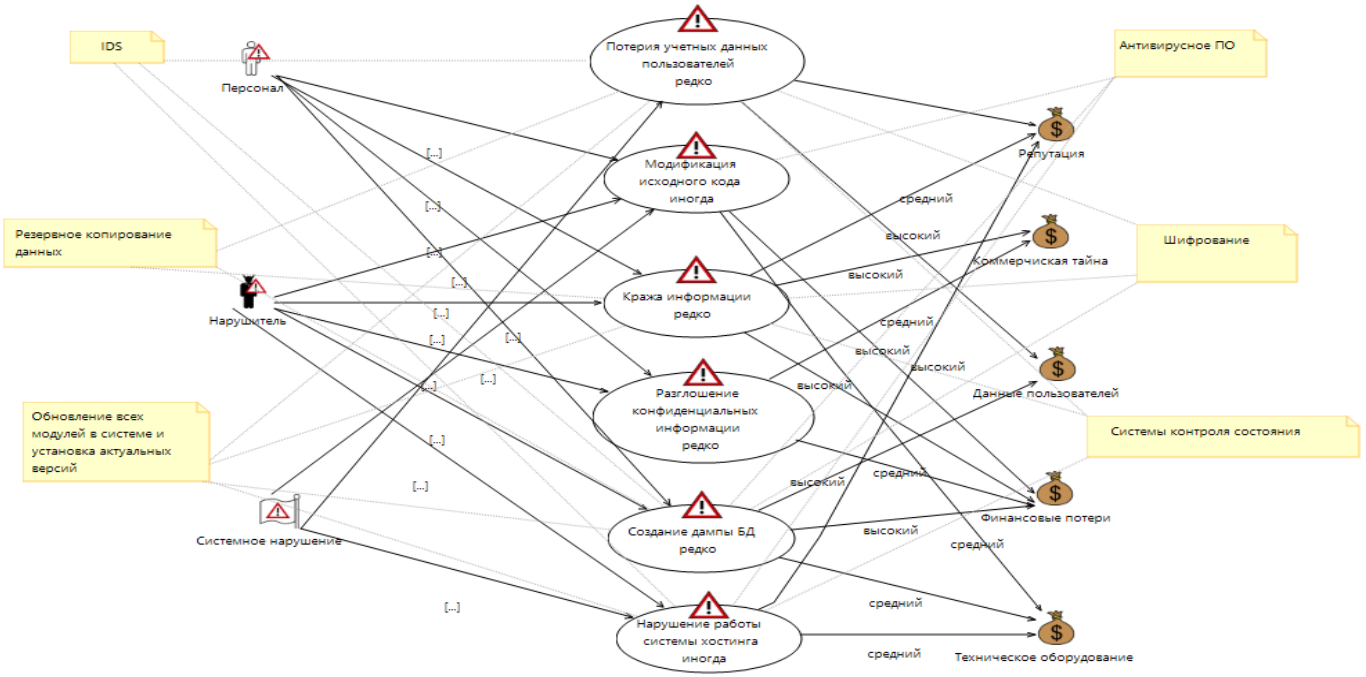
4.4 сурет – Ықтимал сипаттамалары бар қауіптер диаграммасы

Тәуекелдерді азайту барысында активтерімізге шараларды қолданамыз. Яғни, қорғау шаралары осалдықтар және қауіп-қатерлерді жүзеге асу тәсілдері арасында қосылды. 4.5 суреттегі әрбір осалдыққа қарсы іс-әрекеттер көрсетілген.



4.5 сурет – Қорғаныс элементтері бар қауіптер диаграммасы

Жоғарыда көрсетілгендей қорғау шараларын жүзеге асырғаннан кейінде қолайсыз тәуекелдер кездесуі мүмкін. Мұндай жағдайларда шешім қабылдаушылар қолайсыз тәуекелдердің жоғарғы қауіптерді бірінші кезекте жою керек. 4.6 суреттегі диаграммасында қолайсыз тәуекелдер сипатталады.



Сурет 4.6 – Қолайсыз тәуекелдер диаграммасы

4.3 Ақпараттық қауіпсіздік тәуекелдері бойынша қорытынды

Дипломдық жобаның ақпараттық қауіпсіздіктерді анықтау бөлімінде біз веб-сайттың тәуекелдер сипаттамасын анықтадық. Ақпараттық қауіпсіздікті деңгейін жақсарту мақсатында осалдықтар мен тәуекелдер есебі жүргізіліп, оларды жою қызметтері атқарылды.

Веб-сайт негізінде таңдалған активтердің қатерлері мен осалдықтарын қарастырдық. Тәуекелдерді есептеу үшін қос параметрлі есептеу әдісі қолданылды. Есептеу барысында активтерден келетін қолайсыз тәуекелдерді анықтап, қорғану шаралары жүргізілді. Қорғаныс шараларын жүргізу нәтижесінде веб-сайттың қолайсыз тәуекелдерін төмендету жолдары көрсетілді және осының арқасында тәуекелдердің орташа мәні 5-тен 3-ке дейін төмендетілді.

Жобаның екінші бөлімінде Coras жүйсімен тәуекелдерге талдау жүргізілді. Талдау жүргізу барысында UML-графикалық диаграммалары қолданылып, тәуекелдер мен қорғау шараларына сызбалар әзірленді.

5 Өміртіршілік қауіпсіздігі

5.1 Жұмыс жағдайын талдау

Менің диломдық жұмысым мектеп оқушыларына арналған көп салалы курсына сайт жасау болып табылады. Сайтты жазу үшін түрлі программалау тілдері қолданылды және сайттың серверлері көрсетілген 5.1 суретте орналастырылады.

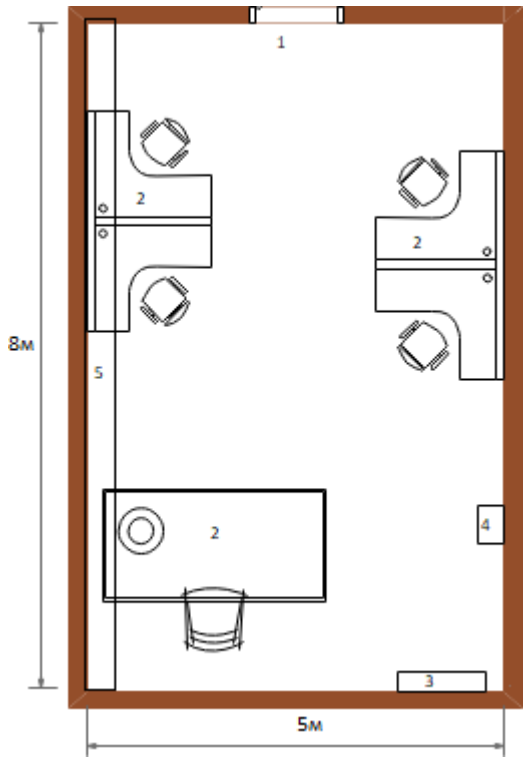
Бөлмеде құрал-жабдықтар мен жұмыс станцияларынан басқа әр түрлі компьютерлер, серверлер, ауа сорғыштар мен желдеткіштер орналасқан. Төменде көрсетілгендей жұмыс барысында компьютерлер орнатылған бөлмеде қызметкерлерге тиеін зақымдар түрлерімен таныс боламыз:

- бөлмелерде терезелер орналаспағандықтан, ауа айналымы ауа сорғыштар мен желдеткіштер көмегімен іске асады. Бірақ желдеткіштер жұмыс барысындар қатты дыбыс шығарады;
- бөлмедегі барлық компьютерлерге дыбысы төмендетілген салқындатқыштар орнатылған. Бірақ серверлерде қуатты салқындатқыштар болғандықтан қызметкерлерге кедергі жасауы мүмкін, болашақта салқындатқыштарды неғұрлым тыныш салқындатқыштарға ауыстыру жоспарда бар;
- барлық жарықтандыру құрылғылары төбеге орналастырылғандықтан, қызметкерлерге ешқандай кедергі тудырмайды;
- электр жабдығымен дұрыс жұмыс істемеген жағдайда 220В соққы алу қауіпі бар;
- компьютердің алдында ұзақ уақыт жұмыс істегендіктен, қызметкерлердің көздері шаршайды, сондықтан болашақта көк түстерді бекітетін көзілдіріктер сатып алу жоспарлануда.

Көрнекі жұмыстарды орындау кезінде 200лк болатын бөлмені қажетті жарықтандыру үшін 12 шамның күшін тексерейік. Жұмыс орнына қалыпты жағдай орнату үшін жарықтандыруды обьектінің көлеміне қарай нормалайды.

Антропогендік қауіптің әсері адамдардың қалыпты өмірін бұзады, төтенше жағдайларға (апаттық жағдайларға) және апаттарға, соның ішінде экологиялық апаттарға әкеледі. Қазіргі уақытта қауіпті табиғи құбылыстар мен процестердің зиянды әсерінің өсуі алаңдаушылық тенденциясына әкеп соқтырды. Белгілі бір елдер мен аймақтардағы барлық нақты жағдайлар үшін олар халықтың өсуіне, салыстырмалы түрде шектеулі аудандардағы оның шоғырлануына және материалдық байлығына, сондай-ақ табиғи апаттар генезисінің сипатының өзгеруіне байланысты пайда болады.

Жұмыс бөлмесінің жоспары 5.1 суретте көрсетілген.



5.1 Сурет – Бөлме

1) Есік
2) Жұмыс орны
3) Желдеткіш
4) Сервер
5) Ауа сорғыш

Бөлме келесі параметрмен орналасқан: - жұмыс орынның өлшемдері: ұзындығы – 3.2 м, ені - 5 м, ұзындығы - 8 м; Жұмыстың визуалды жағдайларына арналған бөлме жарықтық жұмыс санатына жатады (жеңіл физикалық, IA санаты, жұмыс орындықпен жабдықталған және физикалық кернеуді талап етпейді); - жасанды жарықтандыру - шамдар: жарықдиодты шамдар. Компьютермен жұмыс істеу кезінде қауіпті және зиянды факторлар пайда болуы мүмкін, олардың әсері адам ағзасына зиян тигізіп, жарақат алуға әкелуі мүмкін. Негізгі факторлар олардың шығу тегі мен нормалары 5.1 кестеде көрсетілген.

Кесте 5.1 - Қауіптер мен қиянды факторлар

Фактордың атауы	Пайда болуы	Шекті рұқсат етілген деңгейі	Салдары
Электр тізбег кернеуінің өсуі	Әзірлеушінің жұмыс орны	ГОСТ 12.1.038-82. Апаттық режимде ұзақ уақыт әсер ету кезінде ток айналымы Uпр≤36V (1-ден	Электрлі жарақат

		көп).	
Электрлік доға	Тарату қалқаны	ГОСТ 12.2.007.3-75 ГОСТ 12.2.007.4-75 ГОСТ 12.1.004-85	Күік, өрт
Жұмыс аймағының жеткіліксіз жарықтандырылуы	Бөлме	СНиП 23-05 Е=300 Лк	Шаршау, көру қабілетінің нашарлануы
Еңбек монотондылығы	Жұмыс орны	ГОСТ 12.1.003-80	Жүйке психикасының шамадан тыс жұмыс істеуі
Дыбыстың жоғары деңгейі	Жұмыс орны	ГОСТ 12.1.003-88 Жиілік жолақтарының деңгей 75 Дб аспау керек	Есту органдарының зақымдалуы, жүйке психикасының шамадан тыс жұмыс істеуі

5.1.2 Жарықтандыру жүйесі

Бөлменің жарықтандыру жүйесі жобалауы СНиП РК 2.04-05-2002 [3] нұсқаудағы қабылданған жалпы қағидаларға сай келеді.

Жарық адамның өмір сүруінің қажетті шарты болып табылады. Ол жоғары психикалық функциялардың жағдайына және ағзадағы физиологиялық процестерге әсер етеді. Жақсы жарықтандыру сергітеді, жақсы көңіл-күй жасайды, жоғары жүйке қызметінің негізгі процестерінің жұмысын жақсартады.

Спектрлік құрамға байланысты жарық қызықты әсерге ие болады: жылу сезімін күшейтеді (қызғылт-қызыл), тыныштандыратын (сары-жасыл) немесе тежеу (көк-күлгін) процесстерін жүзеге асырады.

Жарық берудің ең маңызды әсері көру функциясына, ал ол арқылы еңбек өнімділігіне әсер етеді. Тиімді жарықтандыру өндірістік жарақаттанудың алдын алуда маңызды рөл атқарады.

Жарақаттанудан басқа, жарықтандырудың қолайсыз жағдайлары қызметкердің көру анализаторының шаршауын тудырады (жүйелі әсер ету кезінде – көру ақауларының дамуы), жұмысқа қабілеттілігін төмендетеді, басқа да ауруларға әкеледі.

Табиғи жарықтандыруда пайда болған жарықтандыру өте кең ауқымда өзгереді. Бұл өзгерістер күн, жыл уақытымен және метеорологиялық факторлармен: бұлттылық сипатымен және жер жамылғысының қасиеттерімен байланысты.

Өндіріс бөлмелерінде жарықтанудың табиғи және жасанды түрлері қолданылады.

Табиғи жарық бөлмеге терезе арқылы түседі. Табиғи жарықтанудың бағалануы табиғи жарықтанудың коэффициенті (ТЖК) бойынша жүргізілінеді.

Жобаның жарық техника бөлімінде жарық сапасының көрсеткішін және жарықтандыру мағынасын, жүйесін, түрін және жарық әдістерін, жарық көздерімен жарық аспаптарын таңдауы орындалады.

Дисплейі бар бөлмелерді жарықтандыру бірқатар талаптарға сәйкес жүзеге асырылады:

- жұмыс бетіндегі және қоршаған кеңістіктегі жарықтылық мүмкіндігінше біркелкі таралады;
- жарықтандыру дұрыс жарық беру үшін жарықтың қажетті спектрлік құрамын қамтамасыз етеді.
- қағаздар, құжаттар және пернетақта аймағында көлденең жазықтықта жарықтандырудың қажетті деңгейі қамтамасыз етіледі;
- экранның тік жазықтығында жарықтандыруды шектеу арқылы дисплейдегі суреттің жарықтандырылуынан сақтандырылады;

5.2 Жасанды жарықтандыруды есептеу

Есеп әдістемелік нұсқауды негізге ала отырып орындалды [1]. Пайдалану анализі әдісімен IT бөлімінің жасанды жарықтандыруын есептеу. Есептеу бөлімі үшін жарықтандыруды, жарық көзін, көрсетілген облысқа немесе жұмыс офисіне шам түрін таңдау қажет. Жұмыс сыныптарын қалыпты жарықтандырумен қамтамасыз ету үшін қажетті жарықтандыруды орнату қуаты мен емін қамтамасыз ету үшін қажетті шамдардың санын анықтау қажет. Көзбен шолу жұмысын тастау. Номиналды жарықтандыру-400 лк. жер беті және басқа да объектілер. Ол ең гигиеналық және адамдар ұзақ уақыт қалатын барлық бөлмелерде қолданылуы керек.

Кесте 5.2 - LED шамдарының техникалық сипаттамалары

Номиналды қуаты, Вт	LED типті шамның номиналды жарық ағыны	Шамның өлшемі, см	
		Диаметрі	Ұзындығы
26	2880	19	4

Шам ретінде YUANFENG cl 29-2 26W / 2880 алынды. Шамның ұзындығы 1900 мм, ені 40 мм. Жасанды жарықтандыруды есептеу, пайдалану коэффициенті әдісімен жүргізіледі. Қабырға мен еден төбесінің көрініс коэффициенттері:

$$\rho\text{ТӨБЕ} = 70\%;\ \rho\text{ҚБ} = 50\%;\ \rho\text{ЕДЕН} = 30\%$$

Жұмыс бетінің үстінде шамды ілу биіктігін есептейміз:

$$H = h - hP - hc, \qquad (5.1)$$

Мұндағы hc- шамнан жабынға дейінгі қашықтық, hc =0,11; hp- еден үстіндегі жұмыс бетінің биіктігі;

hp=0,8 м. h-бөлме ұзындығы, h=3.2 м

H = 3,2 – 0,8 – 0,11 = 2,29м

Терезеден шамға дейінгі тиімді қашықтық төмендегі формуламен анықталады:

$$L = \lambda \cdot H, \quad (5.2)$$

мұндағы λ=1,2 ÷ 1,4;

$$L = 1,2 \cdot 2,29 = 2,748м.$$

Қабырғадан жақын орналасқан шамға дейінгі арақашықтық (жұмыс жүргізілмеген жағдайда) мына формуламен анықтаймыз:

$$l1 = (0,4 \div 0,5) \cdot L, \quad (5.3)$$

$$l1 = 0,4 \cdot 2,748 = 1,1 м.$$

Бөлменің индексін анықтау:

$$i = l*s / H(l+s), \quad (5.4)$$

$$i = 8*5 / 2,29(8+5) = 1,344$$

Бұл жағдайда пайдалану коэффициенті n = 49 тең, қор коэффициенті Кз=1,2 тең.

LED шамдардың санын мына формула бойынша анықтаймыз:

$$S = Ен \cdot Кз \cdot Z \cdot Ат / m \cdot Фл \cdot n, \quad (4.5)$$

мұндағы S- бөлме ауданы, 32; Кз- қор коэффициенті;

Е-берілген минималды жарық, Е=400 лк;

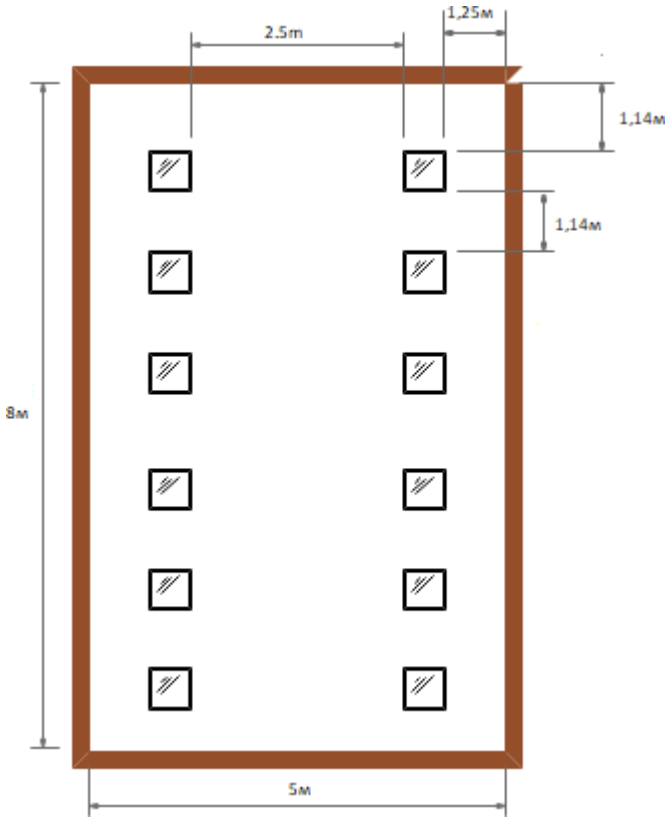
Z- жарықтандырудың біркелкі емес коэффициенті, Z=1,1; m - жарықтандырғыштағы шамдар саны;

Фл- таңдалған шамның жарық ағыны, Фл=2880 лм;

n – қолдану коэффициент, n= 410.

$N = Ен \cdot S \cdot Z \cdot Кз / N \cdot Фл \cdot = 400 \cdot 32 \cdot 1,1 \cdot 1,2 / 1 \cdot 2680 \cdot 0,49 \approx 16896 / 1411 \approx 12$

Барлық жарықтандыру үшін 400 лк - ге 12 шам қажет, әрбір шамның қуаты 26 Вт болуы тиіс, демек, санитарлық нормаларға сәйкес болу үшін қолданыстағы шамдардың санын көбейту немесе азайту қажет емес.



Сурет 5.2 – Шамдарды орналастыру жоспары

Өрт қауіпсіздігі персоналдың жұмыс ортасының қауіпсіздігін қамтамасыз етудегі ҚР ҚНжЕ 2.02-05-2009 [2] сәйкес, ғимарат өрттің даму қауіптілік дәрежесіне, жанғыш материалдардың функционалдық мақсатына және өрт жүктемесіне байланысты 1-ші санаттағы топқа жатады.

Өрттің шығу себебі:

- өңдеу материалдарын ақаулы ажыратқыштардан, розеткалардан от жағу;

- жабдық элементтерін жағу;

- жабдықты пайдалану шарттарын сақтамау;

Өрт болған жағдайда тек бөлме ғана емес, сонымен қатар қымбат құрал-жабдықтар да зардап шегуі мүмкін, сонымен қоса бұл адам өліміне әкеледі. Сондықтан өрттерді анықтау және болдырмау үшін шаралар қолдану қажет. Өрттің пайда болу көздері бұлар: от алдыру көздері, компьютерлердің электрондық схемалары, қызмет көрсету үшін пайдаланылатын құрылғылар, қоректендіру құрылғылары, кондиционерлер болуы мүмкін, онда әр түрлі ақаулардың нәтижесінде пайда болады.

Есеп әдістемелік нұсқауды негізге ала отырып орындалды [4].

Өрт қауіпсіздігі талаптарына сәйкес бөлмеге ОУ-5 отқа төзімді өрт сөндіргіштерді орнатылған. Стандарт бойынша әр 100 м2 бір өрт сөндіргіш орнатылуы тиіс ал, мендегі ғимараттың жалпы ауданы 76,8 м2-ты құрайды сондықтан өрт бір сөндіргіш орнатылған. Өрт сөндіру құралы ретінде көмірқышқыл газы-хладонның аралас қоспасы қолданылады. Көлемді өрт

сөндіру үшін md көміртек-хладон қос тотығының біріктірілген композициясының есептелген салмағы 5.6 шамасымен анықталады:

$$md = k \cdot gn \cdot V, \qquad (5.6)$$

мұндағы k=l,2 – көмірқышқыл-газ хладоның құрамының ескерілмейтін шығындарын өтеу коэффициенті;

gn=0,04 - көмірқышқыл-хладон құрамының нормативтік массалық концентрациясы.

V - бөлменің көлемі мынадай формула бойынша анықталады:

$$V=A \cdot B \cdot H, \quad (5.7)$$

мұндағы A = 8м – бөлме ұзындығы; B = 5м – бөлменің ені;

H = 3,2м – бөлменің биіктігі.

Сонда:

$V = 8 \cdot 5 \cdot 3,2 = 128$ м3.

Демек:

$md = 1,2 \cdot 0,04128 = 6,144$ кг.

х баллондарының есептік саны 12 литрлік 9.5 кг көмірқышқыл-хладон құрамының сыйымдылығы есебінен анықталады.

di магистральдық құбырдың ішкі диаметрі(мм) 4.8 формуласы бойынша анықталады:

$$di=12 \cdot \sqrt{2} =17мм, \quad (4.8)$$

l2 магистральдық құбырдың эквивалентті ұзындығы 4.9 формула бойынша анықталады:

$$l2= k1 \cdot l, \qquad (4.9)$$

мұндағы k1=1,2 - жергілікті шығындарды ескермейтін өтем үшін құбыр ұзындығының ұлғаю коэффициенті;

l=3,2м - жоба бойынша құбырдың ұзындығы, сонда:

$$l2= 1,2 \cdot 3,2=3,84 \text{ м.}$$

Құбырдың эквивалентті ұзындығы мен диаметріне байланысты Q көмірқышқыл-хладон құрамының шығыны 1,4 кг/с тең.

Көмірқышқыл-хладон құрамын берудің есептік уақыты t, 4.10 формуласы бойынша анықталады:

$$t = md /60Q, \qquad (4.10)$$

Сонда,

T = 6.144 / 128·1,4 = 0,0672мин.

Көмірқышқыл-хладон құрамының негізгі қорының салмағы 4.11 формуласы бойынша анықталады:

$$M=1,1 \cdot md \cdot (1+k2 \cdot k1), \quad (4.11)$$

мұндағы k2=0,2 - баллондар мен құбырлардағы көмірқышқыл-хладон құрамының қалдығын ескеретін коэффициент.

Сонда:

$m=1,1 \cdot md \cdot (1+ 0,2/1,2) = 4,72$ кг.

Сонымен, алынған нәтижиелерді автоматты өрт сөндіру жүйесінің қалыпты жұмыс істеуін қамтамасыз ету үшін сыйымдылығы 12 литр көмірқышқыл-хладон құрамының 1 баллоны қажет болады, ал қоспаның салмағы 9.5кг. Газдық өрт сөндірудің автоматты қондырғыларына сәйкес іске қосуға арналған құрылғылары болады.

5.4 Өміртіршілік қауіпсіздігі бойынша қорытынды

Өмір тіршілігінің қауіпсіздігіне талдау жүргізу нәтижесінде өрт ошағының пайда болдырмауына мүмкіндік беретін қауіпсіздік жүйесі әзірленді. Дипломдық жобаның мақсаты оқушылардың қажетті пәндік сабақтарын онлайн түрде оқу үшін web-сайт әзірленді. Бұл жұмыста зерттеу мен әзірлемелердің өзектілігі, компанияның web-сайты онлайн түрде жеке қызықтыратын сұрақтар мен оқушыларға мүмкіндік беретіндігіне негізделеді.

Қорытынды

Берілген дипломдық жоба «Kemel-NT» оқушыларға арналған білім беру орталығының қорғалған веб-сайтын әзірлеуге бағытталған.

Дипломдық жобаны әзірлеу барысында қазіргі таңдағы ақпаратқа төнетін қауіптер мен оның қарапайм адамдарға алып келетін кері әсері жайлы және оны қорғау шараларын ұйымдастыру туралы мәліметтер талқыланды. Сондай-ақ Қазақстан Республикасының ақпараттық қауіпсіздікке арналған заңнамалары мен бұзылған жағдайда жазалау шаралары да қарастырылды.

Веб-сайтты әзірлеу Content Management System мазмұнды басқару технологиясының WordPress платформасында жүзеге асырылды. Веб-сайттың дизайны оқушыларға арнап ыңғайлыстырып әзірленді. Мұнда оқушылар бейнероликтерді көріп, өз араларында пікір-талас ұйымдастыруға сондай-ақ алда болатын сабақтары жайлы мәліметтерді көруге және т. б. мүмкіншіліктері жасалған.

Веб-сайтқа қорғаныс ұйымдастыру жағы қазіргі таңдағы төнетін қауіптерді зерттей отырып керекті жүйлер енгізілді, атап айтқанда:

- Қос факторлы аутентификация;
- Желіаралық қалқан (яғни, брандмауэр және файервол);
- Спам және спам-боттардан қорғау;
- Деректер базасындағы пайдаланушылардың мәліметтерінің қорғалуы сынды сенімді механизмдері ұйымдастырылды;

«Kemel-NT» білім беру орталығының веб-сайты өзінің әсемдігімен және пайдалану қарапайымдылығымен ерекшеленеді.

Әдебиеттер тізімі

1. Система управления (CMS) URL: http://tega.ru/uslugi/sait/cms/ (өтініш күні 27.04.2020)

2. Т. Хассей WordPress. Создание сайтов для начинающих / Т. Хассей. - М.: Эксмо, 2016. - 538 с.

3. Гаспарян А. А. Использование CMS при создании образовательных ресурсов // Учен. зап. : науч. журн. / Курск. гос. ун-т. – 2011. – № 3 (19).

4. PHP-MyAdmin URL: https://php-myadmin.ru/ (өтініш күні 12.02.2020).

5. Костромин В. А. Конспект вебмастера. Выбор системы управления содержанием сайта (контентом) // Справочник вебмастера. – 2009-2013.

6. Методологии управления ИТ-рисками. // www.osp.ru URL: https://www.osp.ru/os/2006/08/3584582/

7. Bjorn, A.G. (January 2002). CORAS, A Platform for Risk Analysis on Security Critical Systems — Model-based Risk Analysis Targeting Security (www.nr.no/coras)

8. Жандаулетова, Ф. Р. Охрана труда: учебник для вузов / Ф.Р. Жандаулетова, Т.Е. Хакимжанов, Т.С. Санатова; МОН РК, НАО АУЭС. – Алматы, АУЭС, 2019. - 399 с.

9. ҚР Құрылыс және тұрғын үй-коммуналдық шаруашылық істері агенттігі: ҚР ҚНжЕ 2.02-05-2009/ Ғимараттар мен имараттардың өрт қауіпсіздігі. Сәулет, қала құрылысы және құрылыс саласындағы мемлекеттік нормативтер: - Астана, 2010. – 107 б.

10. СНиП РК 2.04-05-2002 – «Естественное и искусственное освещение» - Государственные нормативы в области архитектуры, градостроительства и строительства, Астана, 2003

11. Ж.С. Абдимуратов. Охрана труда. Методические указания к выполнению расчетно-графических работ для студентов - бакалавров специальности 5В071800 - «Электроэнергетика» - Алматы: АУЭС, 2013 - 22с

12. Абикенова А.А., Санатова Т.С. Безопасность жизнедеятельности. Методические указания к выполнению раздела «Пожарная профилактика» в выпускных работах для всех специальностей. Бакалавриат - Алматы: АИЭС, 2009. - 32 б.

13. ГОСТ 12.1.003-2014 «Система стандартов безопасности труда. Шум. Общие требования безопасности», Стандартинформ, 2014. - 45б.