ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»
коммерциялық емес акционерлік қоғамы
«Ақпараттық қауіпсіздік жүйелері» кафедрасы

«ҚОРҒАУҒА ЖІБЕРІЛДІ»
Кафедра меңгерушісі с.ғ.к., доцент Бердібаев Р. Ш.
_____ «_____» _____ 2019 ж.
(қолы)

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: «Деректер қорын SQL шабуылдардан қорғау»
Мамандығы: 5В100200 – «Ақпараттық қауіпсіздік жүйелері»
Орындаған: Самуратов Берик. Тобы: СИБк-15-1
Ғылыми жетекші: с.ғ.к., доцент Бердібаев Р. Ш.

Кеңесшілер:
Экономикалық бөлім бойынша:
т.ғ.к., профессор Аренбаева Мс. Г.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «28» 05 2019 ж.
(қолы)

Тіршілік қауіпсіздігі бөлімі бойынша:
аға оқытушы Тлеев Д. Э.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «20» 05 2019 ж.
(қолы)

Есептеу техникасын қолдану бойынша:
т.ғ.к., доцент Шайкулова А.А.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «21» 05 2019 ж.
(қолы)

Мөлшер бақылаушы:
аға оқытушы Аскарова Н.Б.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «05» 06 2019 ж.
(қолы)

Пікір беруші:
т.ғ.к., ассистент-проф
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «31» 05 2019 ж.
(қолы)

Алматы 2019

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«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: Самуратов Берик
(аты-жөні)

Жобаның тақырыбы: Деректер қорын SQL шабуылдарын қорғау

2018 ж. «26» 10 № 124 университет бұйрығымен бекітілді.

Аяқталған жұмысты тапсыру мерзімі: «____»_____20___ ж.

Жобаға алғашқы деректер (талап етілетін зерттеу (жоба) нәтижелерінің параметрлері және зерттеу нысанының алғашқы деректері): Деректер қорын SQL шабуылдан қорғауды іздестіру. Сыналар бойынша шабуылдеу сыртқы көздерін іздестіру. Әртүрлі вирустардан, шабуылдардан қорғану шаралары. Деректер қорын жүзеге асыруға арналған бағдарламалық құралдары іздестіру

Диплом жобасындағы әзірленуі тиіс мәселелер тізімі немесе диплом жобасының қысқаша мазмұны:

1. Деректер қорын жіктеуші
2. Деректер қорына тонетін қауіптерге талдау. Дж қорғау әдістері және құралдары.
3. Дауіп түрлері
4. Шабуыл көздері
5. SQL инъекция
6. PHP инъекция

7. Деректер қорын құру және қорғау
8. Өміртіршілік қауіпсіздігі
9. Техникалық – экономикалық негіздеме
10. Қорытынды

Графикалық материалдардың (міндетті түрде дайындалатын сызбаларды көрсету) тізімі:
1. Деректерді сақтауға оларға қатынас құру бойынша ДҚ жіктелуі
2. Иерархиялық деректер құру
3. Желілік деректер қоры
4. Реляциялық деректер қоры
5. Деректер қорының жіктелуі

Негізгі ұсынылатын әдебиеттер:

1. Баранчиков А. И., Баранчиков П.А., Пылькин А.Н. Алгоритмы и модели доступа к записям БД. – М.: Горячая линия – Телеком, 2011. – 182 с.
2. Поляков А. М. Безопасность Oracle глазами аудитора: нападение и защита. – М.: ДМК Пресс, 2014. – 336 с.
3. Смирнов С.Н. Безопасность систем баз данных. – М.: Гелиос АРВ, 2007. – 352 с.

Жоба бойынша жобаның бөлімдеріне қатысты белгіленген кеңесшілер

Бөлімдері	Кеңесшілері	Мерзімі	Қолы
Экономика	Арендаева Ж.Г.	04.03 – 28.05.19	[signature]
Өміртіршілік қауіп.	Тоқтаев Э.Э.	08.04 – 20.05	[signature]
	Шайкулова А.А.	11.02 – 29.05	[signature]

Диплом жобасын дайындау
КЕСТЕСІ

Бөлімдердің атауы, әзірленетін мәселелердің тізімі	Ғылыми жетекшіге ұсыну мерзімдері	Ескерту
1. Тақырыпты салаға шолу	11.02.2019	
2. Деректер қорын жобалау.	12.02.2019	
3. SQL Server Management studio ортасының негізгі мүмкіндіктері	27.02.2019	
4. Деректер қорына төнетін қауіптер түрлері, олардан қорғану әдістері	14.03.2019	
5. Деректер қорларын жасау және өзгерістер енгізу	22.03.2019	
6. Деректер қорын құру	10.04.2019	
7. Компьютердің ақпарат қорын ұрлаудан қауіпсіздігі	24.04.2019	
8. Өмір тіршілік қауіпсіздігі	20.05.2019	
9. Техникалық - экономикалық негіздеме	28.05.2019	
10. Қорытындының жұмыс қатынысы	29.05.2019	

Тапсырманың берілген уақыты «_____» _____ 20___ж.

Кафедра меңгерушісі _____ (_____)
(қолы) (аты-жөні)

Жобаның
ғылыми жетекшісі _____ (Шайкунова Ә.А.)
(қолы) (аты-жөні)

Орындалатын тапсырманы
қабылдаған студент _____ (Самуратов Б.С.)
(қолы) (аты-жөні)

АҢДАТПА

Дипломдық жоба деректер қорын SQL-шабуылдан қорғауға арналған. Жобада Деректер қорына, олардың құрылымдарына түсінік беріледі, сонымен қатар SQL Server Management Studio ортасының негізгі мүмкіндіктері (SSMS) қарастырылады. Деректер қорына төнетін қауіптерге талдау жасай отырып, соның ішінде SQL-инъекция арқылы төнетін қауіптен қорғану шарасы қамтылады. SQL-инъекциядан деректер қорын қорғау үшін ДҚ әкімшілендіру жағына күш салынады, сонымен қатар ДҚ-ды тестілеу процесі арқылы оның сенімді қорғалғандығы тексеріледі.

АННОТАЦИЯ

Дипломный проект предназначен для защиты базы данных от SQL-атаки. В проекте рассматривается понятие базы данных, их структуры, а также рассматриваются основные возможности среды SQL Server Management Studio (SSMS). В базе данных, анализируя угрозы, угрожающие базам данных, в том числе путем SQL-инъекции, охватывается защита от угроз. Для защиты базы данных от SQL-инъекций предпринимаются усилия в сторону администрирования БД, а также проверяется надежность его защиты через процесс тестирования БД.

ANNOTATION

The Capstone project is designed to protect databases from SQL injection attacks. The project provides the concept of a database, its structure, and discusses the main features of SQL Server Management Studio (SSMS). In a database, analyzing the threats that threaten databases, including SQL-injection, is covered by the threat protection. To protect the database from SQL injections, efforts are made towards database administration, as well as checking the reliability of its protection through the database testing process.

Мазмұны

Кіріспе

SQL-инъекция – бұл зиянкестер зиянды кодты сәтті қалыптастырып, ендіретін деректер қорына бағытталған шабуыл түрі. Өз кезегінде бұл жолдар синтаксистік талдау және орындау үшін деректер қорын басқару жүйесінің серверіне (ДҚБЖ) таратылады. Осы шабуыл сәтті орындалған жағдайда қаскүнем қосымшаның қауіпсіздік жүйесін оңай еңсере алады, деректер қорында (ДҚ) қамтылған құпия ақпаратқа қол жеткізуге, көшіруге, жоюға және өзгертуге болады. ДҚБЖ функционалдық мүмкіндіктеріне де қауіп төндіреді. Кейбір жағдайларда деректер қорын басқару жүйесі жұмыс істейтін сервердің операциялық жүйесіне (ОЖ) кіруге болады. Бұл жағдайда қаскүнем деректер қорында сақталатын құпия ақпаратқа қол жеткізуге, сондай-ақ ДҚБЖ серверінің операциялық жүйесінің командаларын орындауға мүмкіндік алады. Осылайша, серверді келесі шабуылдарға арналған алаңға айналдыруға болады. Мысалы, ұйым желісіндегі басқа қолданбаларды немесе серверлерді шабуылдауға болады.

Әдетте SQL-инъекциялар түріндегі шабуылдарды web-қосымшаларға қатысты қарайды, алайда бұл осалдыққа деректер қорын басқару жүйелерімен жұмыс істейтін кез келген клиент-серверлік және сервистік-бағытталған қосымшалар ұшырайды.

Бұл осалдықтың бұрыннан бар екеніне қарамастан, SQL-инъекциялар салдарынан ақпараттық жүйелерге рұқсатсыз қол жеткізуге және құпия ақпараттың жайылуына байланысты жағдайлардың саны жыл сайын ұдайы өсуде. Ақпараттық қауіпсіздік саласындағы көптеген әзірлеушілер мен мамандар осы осалдықтың маңыздылығын бағаламайды, осылайша ақпараттық жүйелердің қауіпсіздігіне елеулі қауіп төндіреді. Өкінішке орай, бұл тақырып бойынша әдебиетте не туралы жазылса, тек SQL-инъекцияны іске асырудың қарапайым және тривиальды мысалдарына ғана қатысты мәселелер көтеріледі.

Қазіргі уақытта деректер қорынсыз бірде бір мекеме, ұйым, компаниялар жұмыс істемейді. Қоғамның негізгі қызмет функциясы осы деректер қорымен байланысты. Олай болса деректер қорының қауіпсіздігі де өзекті. Бұл салада мамандандырылған компаниялар қауіпсіздік жабдықтарын, әдістерін әзірлеп, деректерге және деректер қорына жасалатын шабуылдарды, оған төнетін қауіптерді талдауда үздіксіз жұмыс атқарып келеді. Тақырыптың өзектілігі тақырыптық саланы зерттеу кезінде деректер қорын басқарудың және олардың бір-біріне әсерін ескерместен қауіпсіздікті қамтамасыз етудің жекелеген аспектілері қозғалады. Бұл жұмыстың зерттеу тақырыбы деректер қорының қауіпсіздігін қамтамасыз ету және әкімшілік ету механизмдері болып табылады. Зерттеу объектісі қауіпсіздікті басқару мен қамтамасыз етуге байланысты ақпараттық процестер болып табылады. Зерттеудің негізгі мақсаты – ДҚ қауіпсіздігін қамтамасыз ету және әкімшілендіру үдерістерінің үзілмеуін көрсету, қолданыстағы әкімшілік құралдарын талдау және қолжетімділікті басқару, қазіргі уақытта бар қолжетімділікті басқарудың оңтайлы моделін таңдау. Жұмыста қойылған мақсат келесі міндеттерді

шешуге себепші болды: 1. Деректер қорының түсінігіне сипаттама беру және жіктелуін сипаттау. 2. Деректер қорының қауіпсіздігін талдау. 3. ДБ әкімшілендіруді қарастыру.

1 Тақырыптық салаға шолу

1.1 Деректер қоры деген не?

Деректер қоры – объективті түрде ұсынылған дербес материалдардың (мақалалар, есептер, нормативтік актілер, сот шешімдері және басқа да ұқсас материалдар) жиынтығы, бұл материалдар электрондық есептеу машинасының көмегімен табылуы және өңделуі мүмкін.

Анықтамаларда келесі ерекшелік белгілер жиі айтылады:

- ДҚ есептеу жүйесінде сақталады және өңделеді;
- осылайша, кез келген компьютерден тыс ақпарат қоймалары (мұрағаттар, кітапханалар, картотекалар және т.б.) мәліметтер қоры болып табылмайды;
- деректер ДҚ-да Есептеу жүйесінде оларды тиімді іздеу және өңдеу мүмкіндігін қамтамасыз ету мақсатында логикалық құрылымдалған (жүйелендірілген).

Әртүрлі өлшемдер бойынша ерекшеленетін деректер қорының көптеген түрлері бар. Мысалы, "деректер қоры технологияларының энциклопедиясында" оның 50-ден астам түрі анықталады [1].

1.2 Деректер қорының жіктелуі

Тұрақты сақтау ортасы бойынша жіктеу:

- екінші жадта немесе дәстүрлі (ағылш . conventional database): тұрақты сақтау ортасы — перифериялық энергияға тәуелді жады (екінші жады), әдетте қатты диск;
- ДҚБЖ жедел жадына тек кэш пен ағымдағы өңдеуге арналған деректер орналастырылады;
- жедел жадта (ағылш . in-memory database, memory-resident database, main memory database): барлық деректер орындау сатысында жедел жадыда;
- үшінші жадта (ағылш . tertiary database): тұрақты сақтау ортасы-әдетте магниттік таспалар немесе оптикалық дискілер негізінде серверден ажыратылатын жаппай сақтау құрылғысы (үшінші жады);
- сервердің екінші жадында тек үшінші жадының деректер каталогы, файлдық кэш және ағымдағы өңдеуге арналған деректер сақталады; деректерді жүктеу арнайы процедураны қажет етеді [1].

Мазмұны бойынша жіктеу

- географиялық;
- тарихи;
- ғылыми;
- мультимедиялық;
- клиенттік.

Үлестірілу дәрежесі бойынша жіктеу:

- орталықтандырылған немесе шоғырланған (ағылш. centralized database): бір компьютерде толық қолдайтын ДҚ;

- үлестірілген ДҚ (ағыл. distributed database) - құрамдас бөліктері қандай да бір критерийге сәйкес компьютерлік желінің түрлі желілерінде орналастырылады;

- біртекті емес (ағыл. heterogeneous distributed database): желінің әр түрлі тораптарында бөлінген ДҚ фрагменттері бір ДҚБЖ-дан астам құралдармен қолдау көрсетіледі;

- біртекті (ағылш. homogeneous distributed database): фрагменттері бөлінген ДҚ желінің әртүрлі түйіндерінде қолдау құралдарымен бір ДҚБЖ-мен байланысқан;

- фрагменттелген немесе секцияланған (ағылш. partitioned database): деректерді тарату әдісі фрагменттеу (топтау, секциялау) арқылы ұйымдастырылған, тік немесе көлденеңінен;

- тираждалған (ағылш. replicated database): деректерді тарату әдісі тираждау (репликация) болып табылады [1].

Сақталатын ақпарат типі бойынша ДҚ-ның жіктелуі:

- құжаттық;
- фактографиялық;
- лексикографиялық.

Құжаттық ДҚ арасында библиографиялық, рефераттық және толық мәтінді болып бөлінеді.

Лексикографиялық дерекқорларға әртүрлі сөздіктер (классификаторлар, көптілді сөздіктер, сөз негіздерінің сөздіктері және т.б.) жатады.

Фактографиялық түрдегі жүйелерде ДҚ-да "фактілер" түрінде тақырыптық облыстың пайдаланушыны қызықтыратын объектілері туралы ақпарат (мысалы, қызметкерлер туралы өмірбаяндық деректер, өндірушілер мен т.б. өнім шығару туралы деректер) сақталады; пайдаланушының сұрауына жауап ретінде оны қызықтыратын объект (объектілер) туралы талап етілетін ақпарат немесе іздестірілетін ақпараттың ДБ-да бар-жоқ екендігі туралы хабарлама беріледі [2].

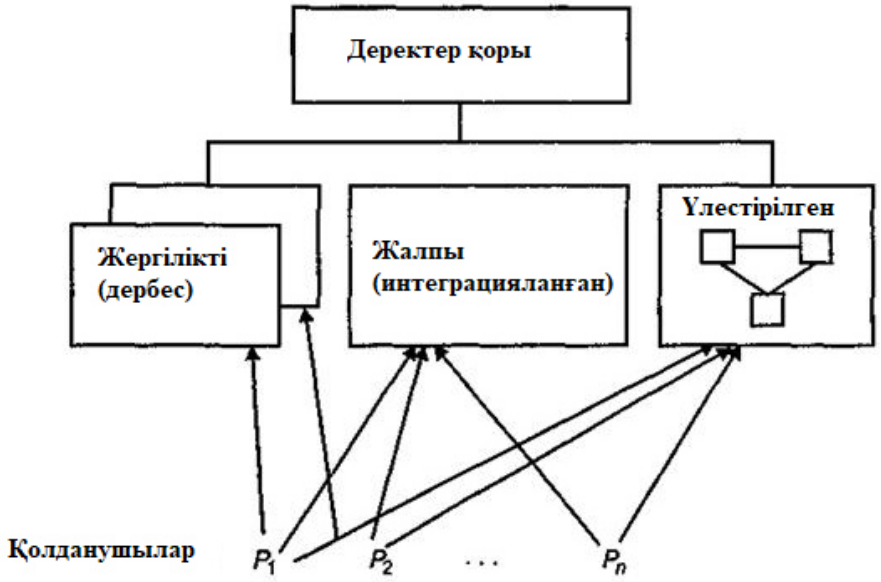
Құжаттық ДҚ-да сақтау бірлігі қандай да бір құжат болып табылады (мысалы, заң немесе мақала мәтіні) және пайдаланушыға оның сұрау салуына жауап ретінде құжатқа сілтеме немесе ол өзін қызықтыратын ақпаратты таба алатын құжаттың өзі беріледі. Құжаттық типтегі ДҚ әртүрлі ұйымдастырылуы мүмкін: сақтаусыз және машиналық тасымалдағыштарда ең бастапқы құжатты сақтаумен. Бірінші типтегі жүйелерге библиографиялық және реферативтік ДҚ, сондай-ақ ақпарат көзіне жіберілетін ДҚ-көрсеткіштерді жатқызуға болады. Құжаттың толық мәтінін сақтау көзделген жүйелер толық мәтінді деп аталады. Құжаттық түрдегі жүйелерде іздеу мақсаты құжаттарда сақталатын қандай да бір ақпарат қана емес, құжаттардың өздері де болуы мүмкін. Іздеу критерийіне белгілер ретінде құжаттардың "құжатты қабылдау күні", "кім қабылдады" және басқа да "шығыс деректері" енгізіледі. Деректер қорының ерекше түрі құжаттар нысандарының деректер қоры болып табылады. Олар құжаттық жүйелердің кейбір белгілері (нақты объект туралы ақпарат емес, құжат іздестіріледі, құжат нысаны әдетте оны іздеу жүзеге

асырылатын атауы болады) және ерекше спецификациялары (құжат одан ақпарат алу мақсатында емес, оны үлгі ретінде пайдалану мақсатында іздестіріледі) бар.

Соңғы жылдары Ақпараттық жүйелерді құруда объектіге бағытталған тәсіл белсенді дамып келеді. Объектілік деректер қоры объектілер және соларға сілтемелер ретінде ұйымдастырылған. Объект осы деректермен операциялар жүзеге асырылатын деректер мен ережелерді білдіреді. Объект объектіні анықтаудың бір бөлігі болып табылатын және объектімен бірге сақталатын әдісті қамтиды. Объектілік деректер қорында деректер кластар типтері бойынша жіктелген және кластардың иерархиялық тобына ұйымдастырылған объектілер ретінде есте сақталады. Класс – қасиеттері бірдей объектілер жиынтығы. Объектілер класқа жатады. Кластар иерархияда ұйымдастырылған(1-сурет).

Деректерді сақтауды ұйымдастыру және оларға қатынас құру сипаты бойынша былай жіктеледі [2]:

- жергілікті (дербес);
- жалпы (интеграцияланған, орталықтандырылған);
- үлестірілген деректер қоры.



Сурет 1 – Деректерді сақтау, оларға қатынас құру бойынша ДҚ жіктелуі

Дербес деректер қоры – бұл бір пайдаланушының жергілікті пайдалануына арналған деректер қоры. Жергілікті ДҚ әрбір пайдаланушы дербес құра алады, және де жалпы ДҚ-дан алынуы мүмкін.

Интеграцияланған және таратылған ДҚ бірнеше пайдаланушылардың бір уақытта бір ақпаратқа (көп пайдаланушы, параллель қол жеткізу режимі) жүгіну мүмкіндігін болжайды. Бұл оларды жобалау кезінде және ДҚ пайдалану процесінде ерекше проблемалард туындатуы мүмкін. Сонымен қатар, ДҚ физикалық түрде әр түрлі бөліктері әртүрлі ЭЕМ-де орналасуы

мүмкін, ал логикалық түрде, пайдаланушының көзқарасы бойынша олар біртұтас болуы тиіс [2].

ДҚ көлемі бойынша жіктеледі. Мұнда өте үлкен деректер қоры ерекше орын алады. Бұл үлкен деректер қоры үшін ақпаратты сақтау тиімділігін қамтамасыз ету және оны өңдеуді қамтамасыз ету мәселелерінің басқаша қойылатындығына байланысты. Деректерді ұйымдастыру сипаты бойынша ДҚ былай бөлінеді:

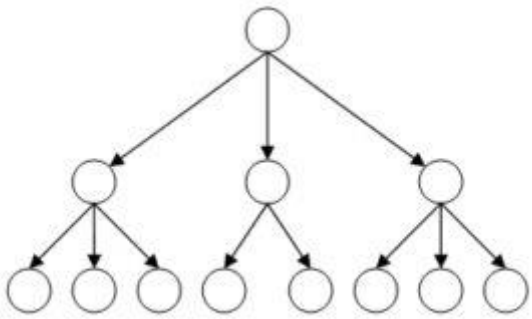
- құрылымдық емес;
- ішінара құрылымдалған;
- құрылымдық.

Бұл жіктеу белгісі символдық түрде берілген ақпаратқа жатады. Құрылымдық емес ДҚ-ға семантикалық желілер түрінде ұйымдастырылған ДҚ-лар жатқызылуы мүмкін. Деректер қорын қарапайым мәтін немесе гипермәтіндік жүйе түрінде ішінара құрылымдалған деп санауға болады. Құрылымдық ДҚ алдын ала жобалауды және ДҚ құрылымын сипаттауды талап етеді. Тек осыдан кейін мұндай түрдегі деректер қоры деректермен толтырылуы мүмкін. Құрылымдалған ДҚ, өз кезегінде, қолданылатын модель түрі бойынша былай бөлінеді.

- иерархиялық;
- объектілік және объектілік-бағытталған;
- объектілі-реляциялық;
- реляциялық;
- желілік;
- функционалдық топ.

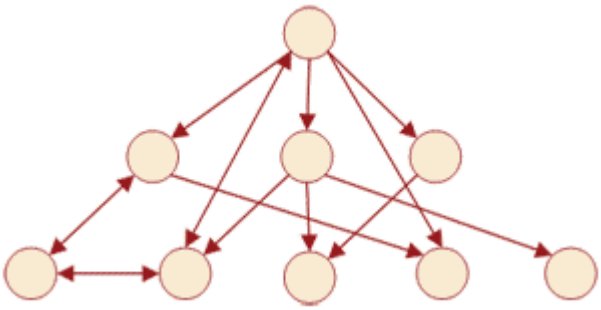
Модель типі бойынша жіктеу деректер қорына ғана емес, ДҚБЖ-не де қатысты [3].

Иерархиялық деректер қоры – әрбір объект осындай жағдайда ақпаратты сақтаудың белгілі бір объектісі түрінде ұсынылады, яғни бұл мәнде туынды элементтер, туындатушы элементтер болуы мүмкін, ал олардың еншілес элементтері болуы мүмкін, бірақ барлығы басталатын бір объект бар. Оны бұтақ түрінде көрсетуге болады(2-сурет):



Сурет 2 - Иерархиялық деректер құры.

Желілік деректер қоры – иерархиялық деректер қорының өзіндік модификациясы болып табылады. Егер сіз жоғарыда суретті мұқият қарап отырсаңыз, онда әрбір төменгі элементке жоғарғы элементтен тек бір көрсеткіш бар екенін көруге болады. Яғни, иерархиялық деректер қорында әрбір еншілес элементте тек бір туынды элемент болуы мүмкін. Желілік деректер қорларында бір туындатушы элементер бірнеше туынды элементтермен байланысуы мүмкін, яғни өзінен жоғары тұрған бірнеше элементтен ортақ қасиет иемденуі мүмкін(3-сурет) [3]:



Сурет 3 – Желілік деректер қоры

Реляциялық деректер қоры – реляциялық деректер моделіне негізделген деректер қоры. Ол өте кең таралған, ол математикада жеңіл баяндалады(4-сурет).

Сурет 4 – Реляциялық деректер қоры

Құрылымдар өте қарапайым болып көрінгенімен, іс жүзінде негізгі деректер қорының құрылымы бірнеше есе күрделі болуы мүмкін. Айтылғандарды қорытындылай келе, деректер қорларының жіктелуін мынадай түсінікті құрылымда көрсетуге болады(5-сурет) [3].

Сурет 5 – Деректер қорының жіктелуі

1.3 Деректер қорын жүзеге асыруға арналған бағдарламалық құралдарға шолу

Қазіргі уақытта әлемде әмбебап өнеркәсіптік ДҚБЖ айтарлықтай көп қолданылады. Олардың арасында технологиялардың даму деңгейі бойынша да, нарық көлемі бойынша да бірнеше күмәнсіз көшбасшыларды атап өтуге болады олар ДҚБЖ әлемдік нарығының 90% - дан астамын алып отыр. Бұл бірінші эшелонның ДҚБЖ – Oracle, Microsoft SQL Server, MySQL, Microsoft Access және IBM DB2, соңғы уақытта PostgreSQL ашық коды бар жүйе. Екінші эшелонның ДҚБЖ тізімі өте үлкен, мұнда Sybase, Informix, Ingress, Adabas, Interbase, Progress, Cache, Linter, Firebird, Teradata және т.с.с. [4].

Ең көп таралған ДҚБЖ егжей-тегжейлі қарастырайық.

1) Oracle ДҚБЖ. Бұл серверге маңызды талаптар қоятын, корпорация деңгейінің деректер қорын жүзеге асыруға арналған ең қуатты қазіргі заманғы ДҚБЖ-ның бірі. Oracle көптеген операциялық жүйелерде жұмыс істей алады: Windows-NT, -2000, Linux, UNIX, AIX, Nowell Netware. Oracle-ді ДҚБЖ ретінде пайдалану бағдарламалау тілін таңдауға мүмкіндік береді. Дәстүрлі түрде бұл үшін PL/SQL тілі қолданылады, бірақ Java бағдарламалау тілін әлдеқайда қуатты қолдануға болады. Oracle-де тек бір серверді ғана емес, сондай-ақ ғаламшардың әр түрлі бөліктерінде орналасқан серверлер тобын басқарудың қуатты және ыңғайлы құралдары бар. GPON технологиясының негізгі артықшылықтары: өте үлкен көлемдегі (64 Гбайтқа дейін) деректер қорын қолдау, өңдеу мен әкімшілік етудің қуатты құралдары, көппроцессорлық және екі тілдік орталарды қолдау, сондай-ақ Web-пен үйлесімді деп есептеуге болады. Сонымен қатар Бағдарлама күрделі аппараттық қамтамаларды талап етеді, бағасы жоғары.

2) MS SQL Server-2000 ДҚБЖ әкімшілік қызметтердің кең спектрін ұсынады және оңай масштабталады. Бұл оны орта бизнес үшін ақпараттық жүйелерде және үлкен компьютерлік ақпараттық жүйелерде (КАЖ) пайдалануға мүмкіндік береді. MS SQL Server платформасының негізінде Windows ортасы қолданылады. Программаның басты артықшылығы - Microsoft программалық өнімдерімен тығыз интегарцияланады және деректерді экспорттау/импорттауда деректердің кең таралған форматтарын қолдайды. Бұл MS SQL Server-ді орталық деректер қоймасы ретінде пайдалануға мүмкіндік береді.

3) Borland Interbase ДҚБЖ-де шағын және орта бизнес қажеттіліктеріне арналған ДҚБЖ-дан талап ететін барлық нәрсе бар. Сонымен қатар, 6.0 нұсқасынан бастап бағдарлама тегін болды, бұл да айтарлықтай артықшылық береді. Бағ дарлама аппараттық бөлімге талап қоймайды. Borland Interbase Windows және Linux платформаларымен, сондай-ақ UNIX, NetBSD, FreeBSD платформаларымен жұмысты қолдайды. Delphi, Kylix және C++ Builder сияқты Borland танымал бағдарламалау тілдері осы ДҚБЖ-мен жұмыс істеуге мүмкіндік беретін компоненттермен қамтамасыз етіледі. Бұл бағдарламаның өте жоғары жылдамдығына қол жеткізуге мүмкіндік береді.

4) MySQL ДҚБЖ Интернетте деректер қорымен жұмыс істеу құралы ретінде кең таралған. Бағдарлама жұмыс істейтін сервер ресурстарына талап соншалықты жоғары емес, өте жылдам және сонымен қатар тегін: әртүрлі платформаларға арналған бастапқы кодтар мен дистрибутивтер Интернетте қол жетімді. Бастапқыда бағдарлама Linux операциялық жүйесіне бағытталған, бірақ қазір Windows, UNIX, NetBSD, FreeBSD, AIX операциялық жүйелеріне арналған бағдарламаның нұсқалары бар. Соңғы уақытта бағдарлама Macintosh пайдаланушыларына Mac OSX операциялық жүйесін пайдалана отырып танымал.

5) MS Access ДБЖ шектеулі деректер көлемі бар жергілікті кеңселік тапсырмаларды шешу және жұмыс нәтижелері бойынша есептерді қалыптастыру үшін пайдаланылады, бұл ретте есептер кеңселікк қосымшалар үшін стандартты түрде ұсынылуы мүмкін. MS Access бір уақытта екі тілде бағдарламалау мүмкіндігіне ие(Visual Basic және SQL қатты керілген диалект) және CASE-құралдары бар, сонымен қатар жұмыс нәтижелері бойынша есептерді жасаудың қуатты және көрнекі құралы болып табылады. Бағдарламалық қамтамасыз ету бағдарламаның мәтіні мен күрделі құрылымның реляциялық деректер қоры бар бір файлдан тұратын бағдарламаларды құруға мүмкіндік береді. Access басқа Microsoft шешімдерімен оңай біріктіріледі. Бұл оны серверлік бөлім ретінде әрекет ететін MS SQL Server байланыстыруында ақпараттық кешеннің клиенттік бөлігі ретінде пайдалануға мүмкіндік береді [5].

1.4 SQL Server Management Studio ортасының негізгі мүмкіндіктері (SSMS)

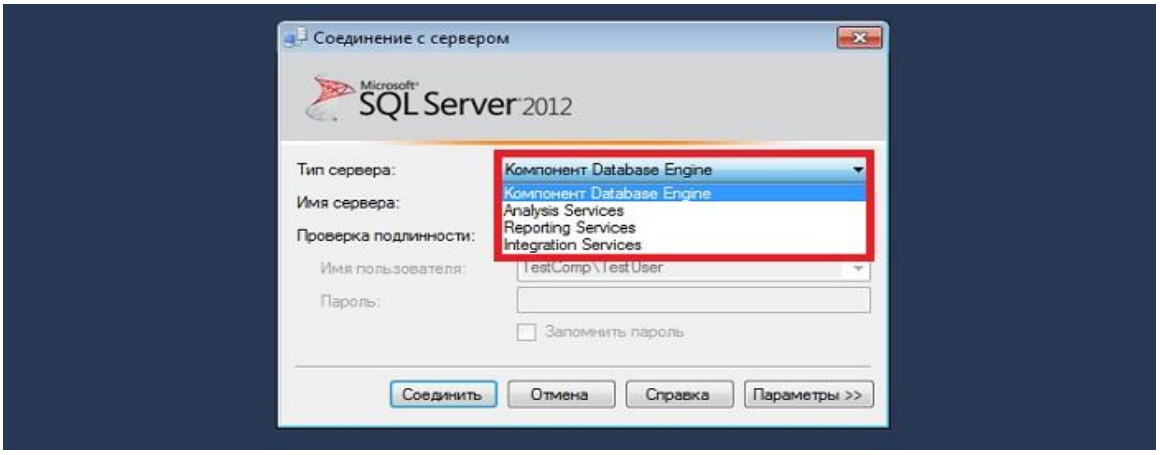
SQL Server Management Studio (SSMS) орта – бұл T-SQL сценарийлерін әзірлеу және SQL Server барлық компоненттерін басқару үшін графикалық құралдар жиынтығы.

Management Studio – кез келген әзірлеуші немесе MS SQL сервер әкімшісінің негізгі құралы.

Егер біреу ертерек шыққан SQL Server нұсқаларымен таныс болса, онда Management Studio бағдарламасында Enterprise Manager, Query Analyzer және Analysis Manager сияқты бағдарламалардың мүмкіндіктері біріктірілген. Қазіргі уақытта Microsoft SQL Server 2005, 2008 нұсқаларын шығаруды толық аяқталды, осыған байланысты, осы және одан ерте шығаруды пайдаланатын барлық қолданушылар сервердің SQL жаңа нұсқаларына өте бастады [5].

Кез келген SQL Server компонентіне қосылу

Management Басқару Studio көмегімен Database Engine, Integration Services, Analysis Services, Reporting Services қызметтері сияқты SQL Server компоненттеріне қосылуға болады(6-сурет).

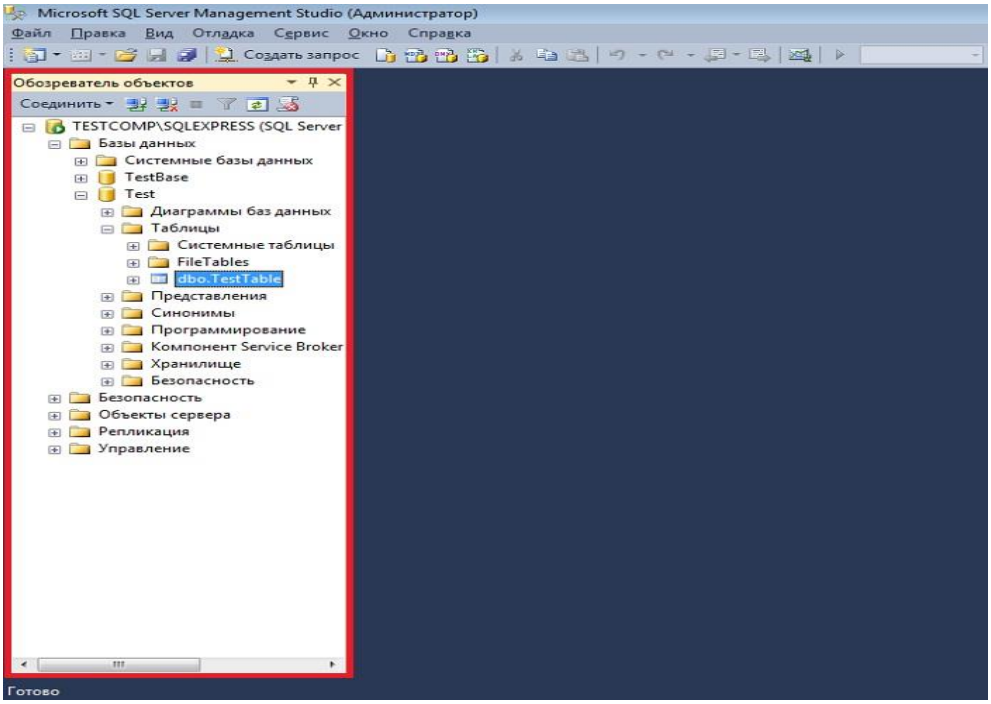


Сурет 6 – SQL Server 2012 ортасында сервермен қосылысты орнату

Басқа сөзбен айтқанда, Management Studio көмегімен Database Engine негізгі компонентін ғана емес, басқа да маңызды компоненттерді басқаруға болады. SQL Server Management Studio-бұл SQL серверін басқару бойынша бірыңғай толық функционалды бағдарлама.

Объектілердің шолушысы

SQL Server Management Studio ортасында барлық сервер нысандарын көруге мүмкіндік беретін және осы нысандарды басқару үшін графикалық интерфейсті ұсынатын нысандар шолушысы бар. Бастау үшін "Вид -> Обозреватель"(7-сурет) мәзірін пайдалануға болады.

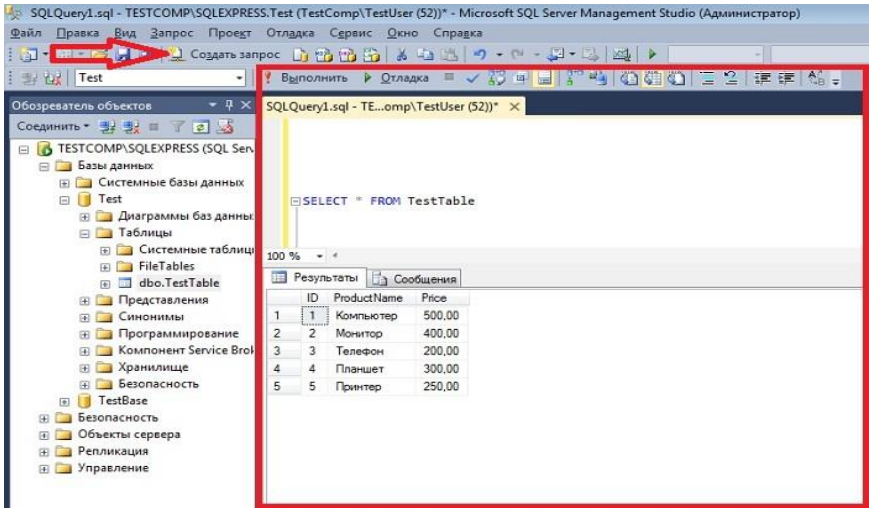


Сурет 7 – Деректер шолушысының көрінісі

Яғни, объектілерді шолушы көмегімен сіз қандай деректер қорын, кестелерді, функцияларды және т. б. көре аласыз; қандай пайдаланушылар құрылған, қандай байланысты серверлер бапталған, осылардың барлығын көруге болады. Сол үшін де ол «Объектілер шолушысы» деп аталады [6].

Сценарийлерді жасау және өңдеу

Бұл мүмкіндік T-SQL-ге сұраныс жасауға немесе скрипттерді жазуға мүмкіндік береді, яғни мұнда барлық SQL нұсқаулықтар жазылады. Егер сіз сервердің SQL деректер қорының бастаушы бағдарламашысы болсаңыз және базаға немесе SQL нұсқауды қайда жазу керектігін білмесеңіз, онда біліңіз, бұл Management Studio код редакторының көмегімен жасалады. Код редакторының терезесін ашу үшін "Сұраныс құру" түймесін басу қажет(8-сурет).

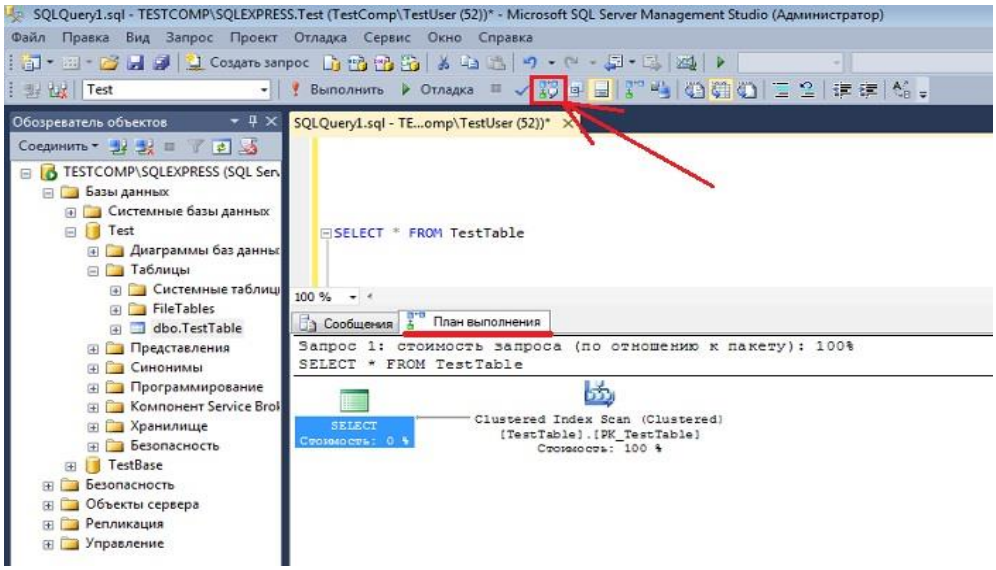


Сурет 8 – Сұраныс құру опциясының мүмкіндігі

Бұл редакторда көптеген мүмкіндіктер бар, мысалы, санаттар бойынша түспен бөлу, яғни код тағайындау. Бұл жоғарыдағы мысалда көрсетілген.

Сұранысты орындау жоспарын қарау

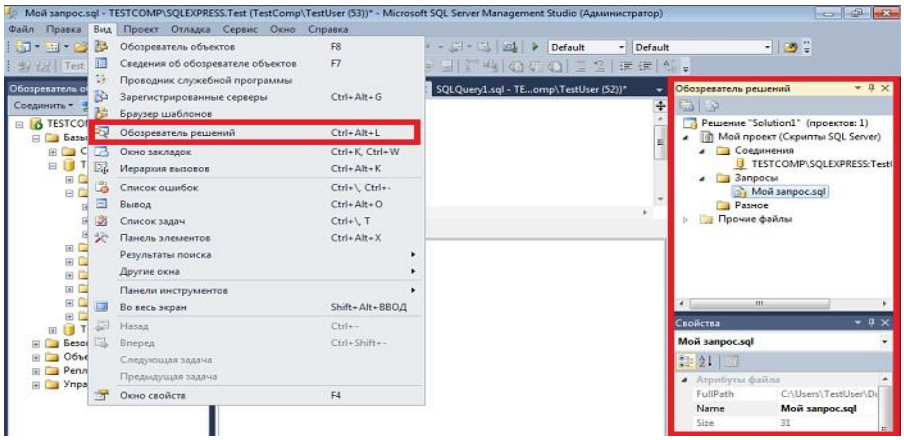
Басқару Studio-дегі сұраныстарды оңтайландыруды жеңілдету үшін код редакторына сұраныстарды орындау жоспарын қарауға мүмкіндік беретін функционал кіріктірілген, және ол оңтайлы болмаса, ол сол немесе басқа индексті құруды ұсынады(9-сурет).



Сурет 9 – сұраныстарды орындау жоспарын қарау

Шешімдер шолушысы

Management Studio – да жүйелендіру, ыңғайлы сақтау және оларға қол жеткізу мақсатында барлық сценарийлерді немесе скрипттерді жобаға топтастыруға болатын функционал бар. Осы шолғышты көрсету үшін "Вид ->Обозреватель решения" түймесін басу қажет(10-сурет) [6].

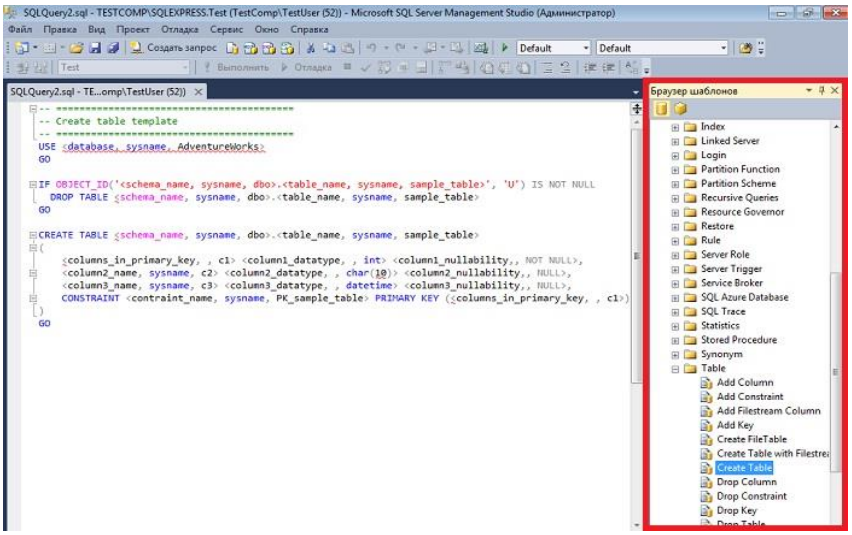


Сурет 10 – Шешімдер шолушысы

Шаблондар шолушысы

SSMS ортасында деректер қоры объектілерін құрудың немесе модификациялаудың типтік сценарийлерін жазуды жеңілдету үшін SQL

нұсқаулықтардың кірістірілген үлгілерін, яғни осы сценарийлердің тақырыптарын пайдалану мүмкіндігі бар. Басқа сөзбен айтқанда, мысалы, кестені жасау немесе өзгерту қажет болса, ал сіз синтаксисті ұмытып кетсеңіз, "Вид ->Браузер шаблонов" (SQL Server 2008 "шаблон шолушысы" деп аталады) (11-сурет) шаблон шолғышын оңай ашуға болады, сәйкес келетін атауды таңдауға және сізге қажетті нысандардың атауларын қоюға болады.

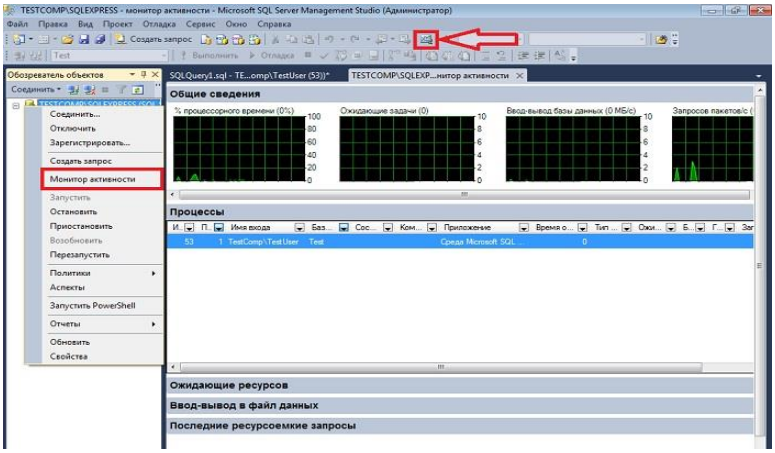


Сурет 11 – Шаблондар браузері

Сондай-ақ, жиі орындалатын тапсырмалар үшін немесе тиісті кірістірілген үлгі жоқ жағдайларда өз үлгілерін жасау мүмкіндігі бар.

SQL Server активтілік мониторы

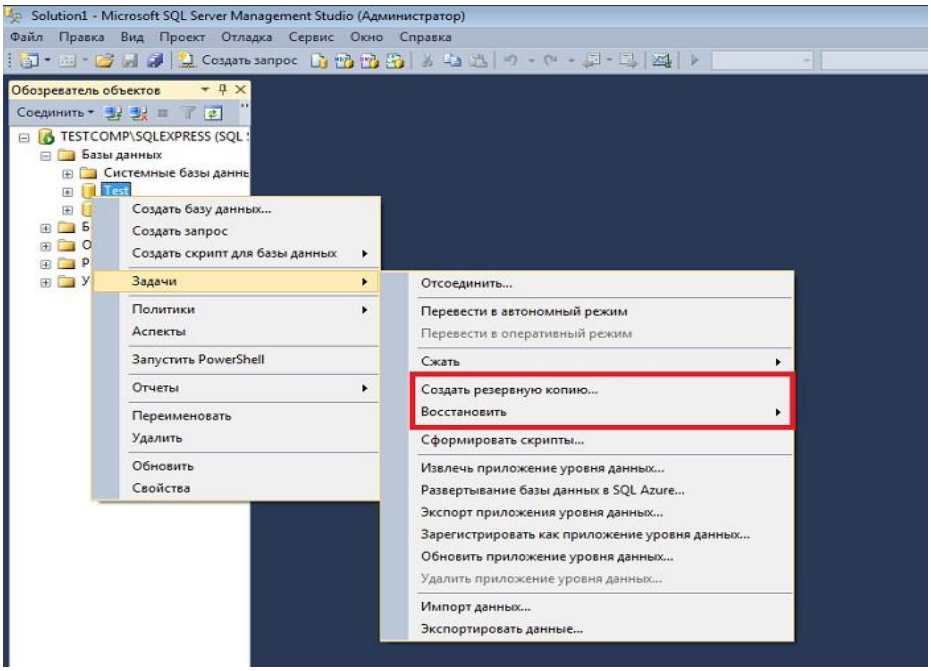
SQL Server Management Studio ортасында "белсенділік мониторы " бар, ол сервердегі ағымдағы белсенділікті бақылауға мүмкіндік береді, мысалы, қазіргі уақытта қандай сұраныстар орындалады, қандай пайдаланушылар қосылған және т.б. Іске қосу үшін нысандар шолғышында сервер бойынша тышқанның оң жақ батырмасын басып, "белсенділік мониторын" таңдауға немесе құралдар тақтасындағы белгішені басуға болады(12-сурет) [6].



Сурет 12 – SQL Server Management Studio ортасындағы «белсенділік мониторы»

Backup деректер қорының сақтық көшірмесін жасау және қалпына келтіру

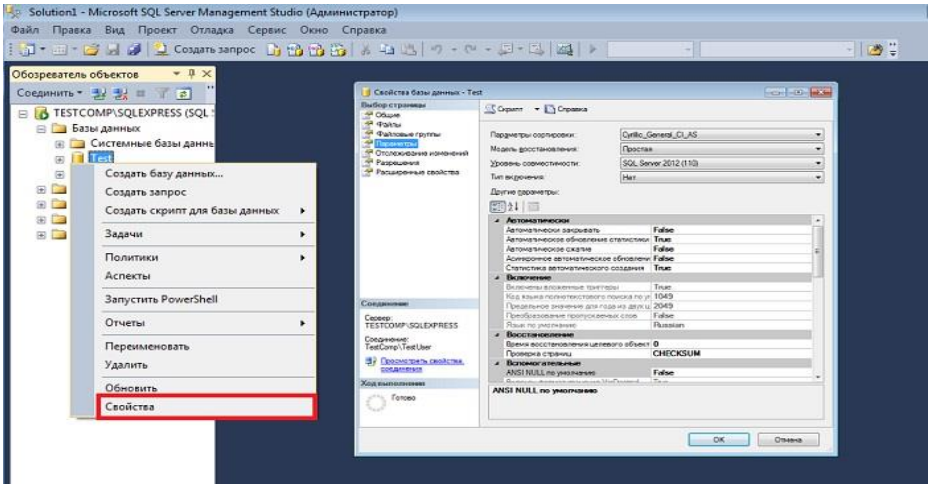
Management Studio көмегімен графикалық режимде деректер қорының сақтық көшірмесін жасау және backup қорларын қалпына келтіру оңай болады. Мұны істеу үшін қажетті деректер қорына тышқанды апарып, оның оң жақ батырмасын басу керек - >есептер - >сақтық көшірмесін жасау / Қалпына келтіру опциясы таңдалатын болады(13-сурет).



Сурет 13 – Резервтік көшірме жасау опциясы

Сервердің, дерекқорлардың және басқа да нысандардың қасиеттерін баптау

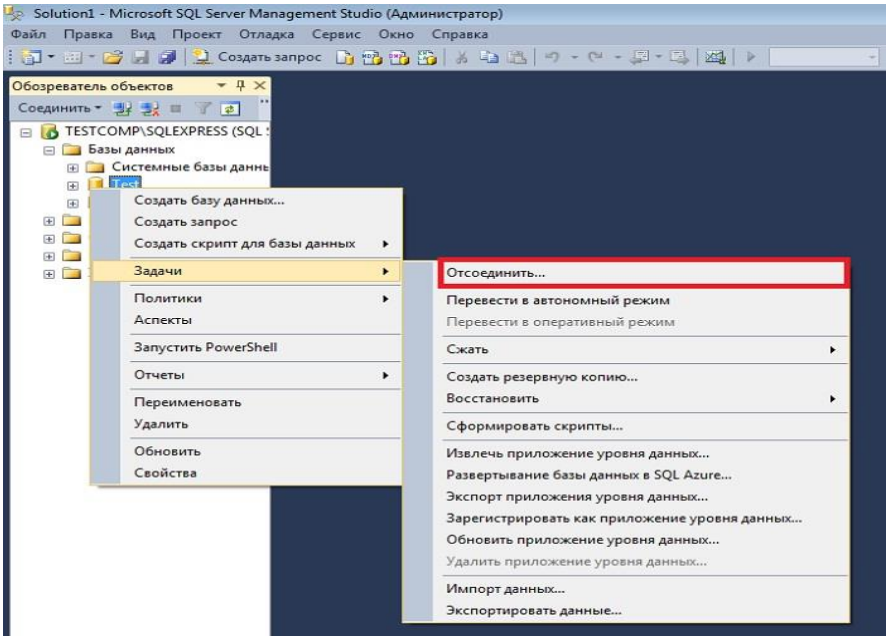
SQL Server Management Studio ортасы сервер қасиеттерін және осы сервер нысандарын өзгертуге мүмкіндік береді. SQL серверінде әрбір объектінің қасиеттері бар, оларды басқаруды Studio графикалық құралдары арқылы өзгертуге немесе көруге болады. Мысалы, деректер қорының сипаттамаларын өңдеу үшін базаны таңдап, тышқанның оң жақ батырмасын басып, «Қасиеттерін» таңдау қажет. Кейбір қасиеттер тек оқу үшін ғана қол жетімді, ал кейбіреулерін өзгертуге болады, мысалы, бұл жағдайда "Параметрлер" бөліміне өтіп, қажетті параметрлерді өзгертуге болады(14-сурет).



Сурет 14 – Қасиеттер опциясының көрінісі

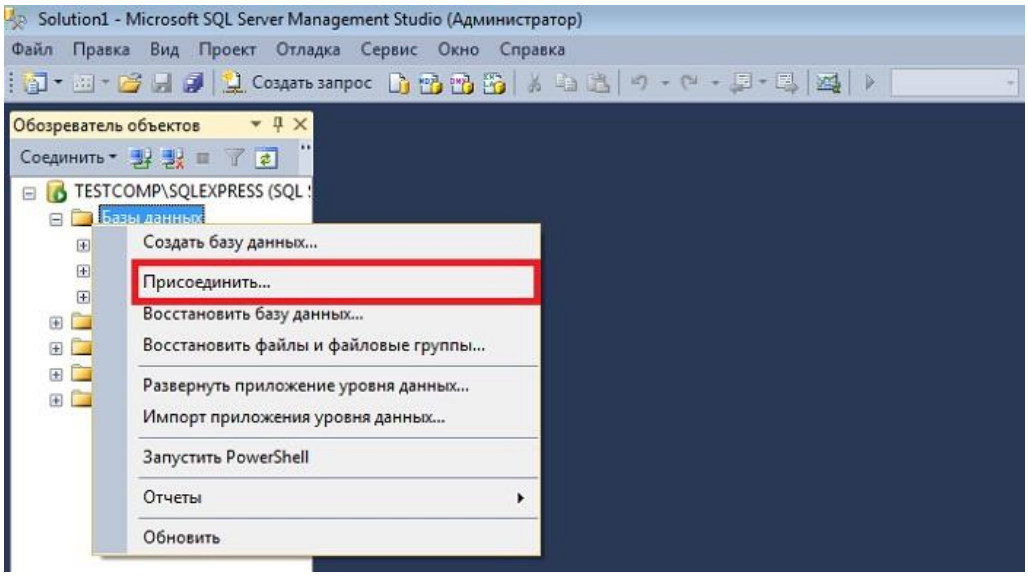
Деректер қорын қосу және ажырату

Management Studio-да деректер қорын қосу және ажырату мүмкіндігі бар. Мысалы, сізде деректер қорын бір серверден екіншісіне көшіру қажеттілігі пайда болды, сондықтан мұны SSMS графикалық құралдары арқылы жасауға болады. Ол үшін Сіз бір серверде деректер қорын сол қорға тышқан нұсқағышын апарып, оң жақ батырмасын басу арқылы ажыратуға болады: опциясы - >Тапсырмалар - >Ажырату(15,16-сурет).



Сурет 15 – деректер қорын қосу және ажырату опциясы

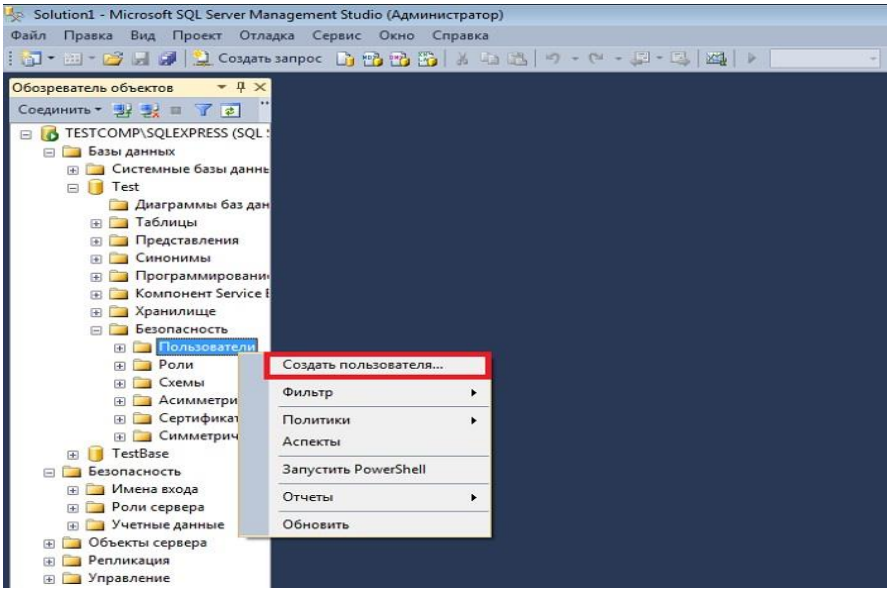
Содан кейін деректер қорының файлдарын жаңа серверге көшіріп, Management Studio-да тышқанның оң жақ батырмасымен басыңыз, қажетті таңдалатын опциялар: «*Базы данных*» және «*Присоединить…*» [7].



Сурет 16 – «*Базы данных*» және «*Присоединить…*» опциясы

Сервердің қауіпсіздігін басқару

SQL Server Management Studio ортасы SQL сервердің қауіпсіздігін басқару мүмкіндігін де қамтыған, яғни серверге, деректер қорының пайдаланушысына кіру атын жасауға немесе сервер объектілеріне кіру мүмкіндігін реттеуге болады. Мысалы, Деректер қорының қолданушысын құру үшін мына опциялар таңдалу керек: Деректер қоры *->Қажетті қор->Қауіпсіздік ->Қолданушылар -> Тышқанның оң жақ батырмасын басу -> Создать пользователя*(17-сурет).

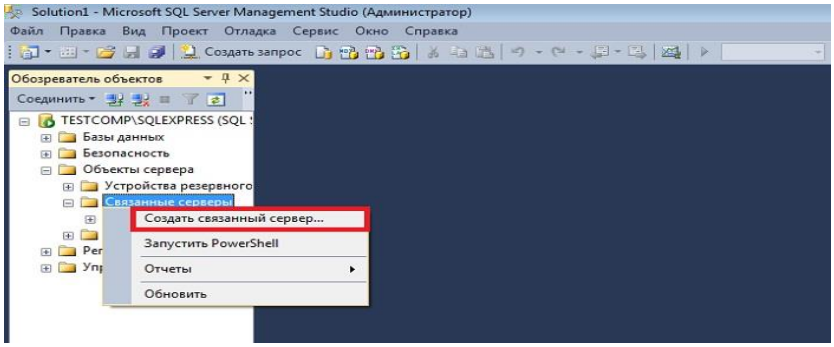


Сурет 17 – Деректер қорының қолданушысын құру

Байланысқан серверлерді құру

Management Басқару Studio-да байланысқан серверлерді жасау үшін графикалық құралдар бар. Егер біреу SQL серверінде "байланысқан серверлер" дегеннің не екенін білмесе, онда "байланысқан серверлер MS SQL

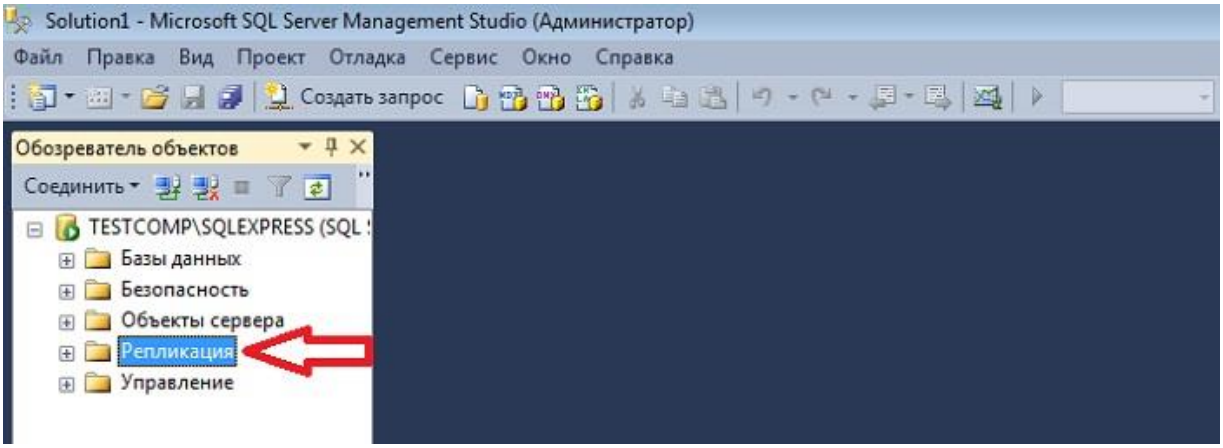
Server" материалын оқуға болады. Бұл мүмкіндік «*Объекты сервера -*>*Связанные серверы*» контейнерінде қолжетімді(18-сурет).



Сурет 18 – Байланысқан серверлер құру опциясы

Деректер қорының репликациясын баптау

Management Studio-да деректер қорын репликациялау үшін графикалық құралдар да бар. Осы мақсаттар үшін "Репликация"атты бөлек контейнер қолданылады(19-сурет).

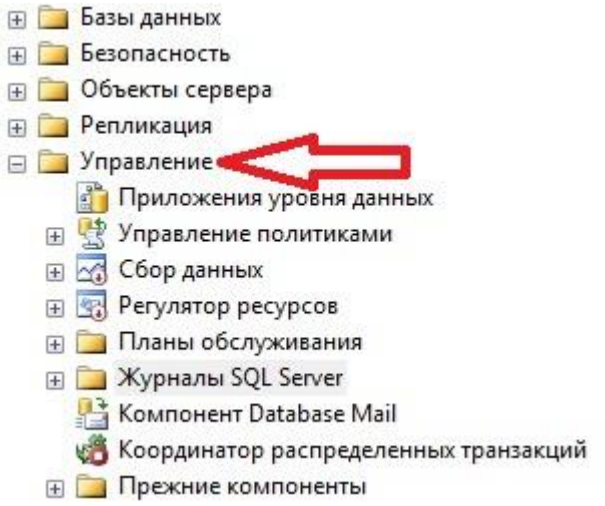


Сурет 19 – Репликация контейнері

Әкімшілік міндеттерді орындау

Management Studio SQL серверін басқару құралы ретінде де әрекет етеді, мысалы, ДҚ қызмет көрсету жоспарын жасауға немесе жүйелік журналдарды көруге болады. Функционал "басқару" контейнерінде қол жетімді(20-сурет).

Ескерту**!** *Express редакциясында SQL серверді басқару бойынша толық функционал жоқ, осыған байланысты төменде Enterprise редакциясында SQL сервердің скриншоты ұсынылған* [7].



Сурет 20 – Әкімшілік қызметтерін жүзеге асыру контейнері

1.5 Management Studio SQL артықшылықтары мен кемшіліктері

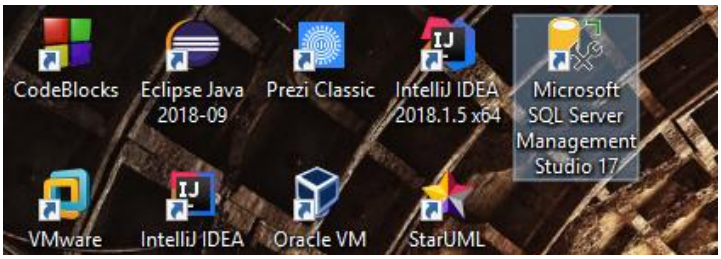
Елеулі кемшілігі – пайдаланушы үшін ДҚБЖ ресурстарының максималды көлемі қаншалықты қол жетімді екенін анықтау қиын (мысалы, 20% - дан артық емес). Нәтижесінде, MS SQL Server пайдаланушыларының бірі ресурстарға талап ететін SQL-сұранымды іске қосса, онда ол барлық қол жетімді ДҚБЖ ресурстарын өзіне алады. Нәтижесінде барлық қалған пайдаланушылар тәуелді (немесе өте баяу жұмыс істейді), немесе тіпті ДҚБЖ-ға қосыла алмайды, яғни бір пайдаланушы барлық басқа қолданушылардың жолын жауып тастайды. Осылайша, MS SQL Server-ді көптеген пайдаланушылар SQL-сұраныс жасайтын ортада немесе ақпараттық жүйелерде пайдалану орынсыз. Басқаша айтқанда, егер сізде бір мезгілде жұмыс істейтін пайдаланушылар 100-ден аз болса және олар индекстерді (қандай да бір бухгалтерия, қойма және т. б.) пайдалана отырып кестелерге үлгі сұраныстарды жіберетін клиенттік қосымшалармен жұмыс істесе, онда SQL Server батыл қолдануға болады.

Артықшылығы – жылдам және жеңіл орнатылып, бапталады. Қолдану, үйрену жеңіл және қарапайым.

Ал егер қолданушылар саны көп болса, сұраныстар күрделі болса үлкен ДҚБЖ-ларды (Oracle және DB2) дұрыс [8].

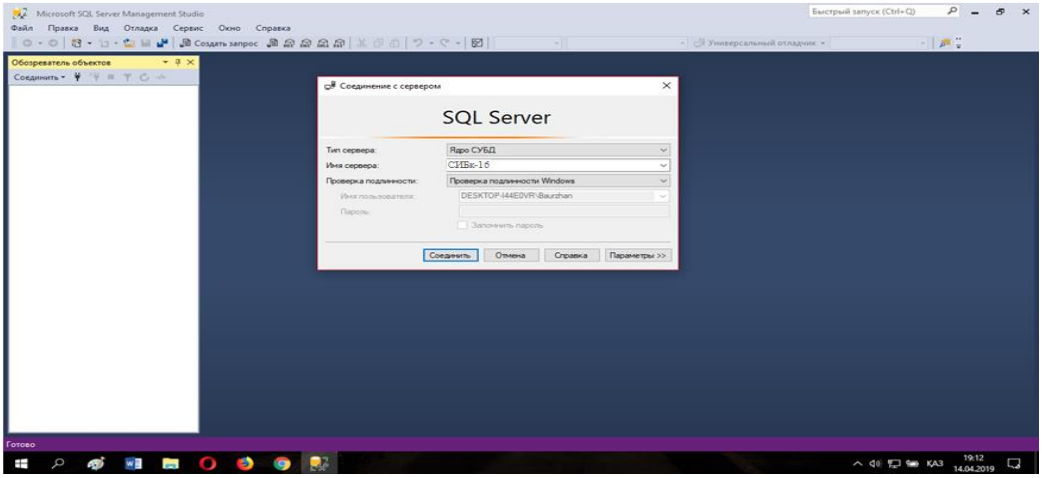
1.6 SQL Server Management Studio программасын орнату және жұмысқа қосу

SQL Server Management Studio (SSMS) – Microsoft SQL Server барлық компоненттерін конфигурациялау, басқару және әкімшілендіру мақсатындағы Microsoft SQL Server 2005 және одан кейінгі версияларынан алынған утилит. Бұл утилит объектілермен жұмыс істеп, серверді баптауға арналған скриптік редактор мен графикалық программаны қамтиды. Программаны https://go.microsoft.com/fwlink/?linkid=2043154 (https://www.microsoft.com/ru-ru/sql-server/sql-server-editions-express) сайтынан тегін орнатуға болады(21-23-сурет).



Сурет 21 – компьютерге орнатылғаннан кейінгі программаның жұмыс үстеліндегі жарлығы

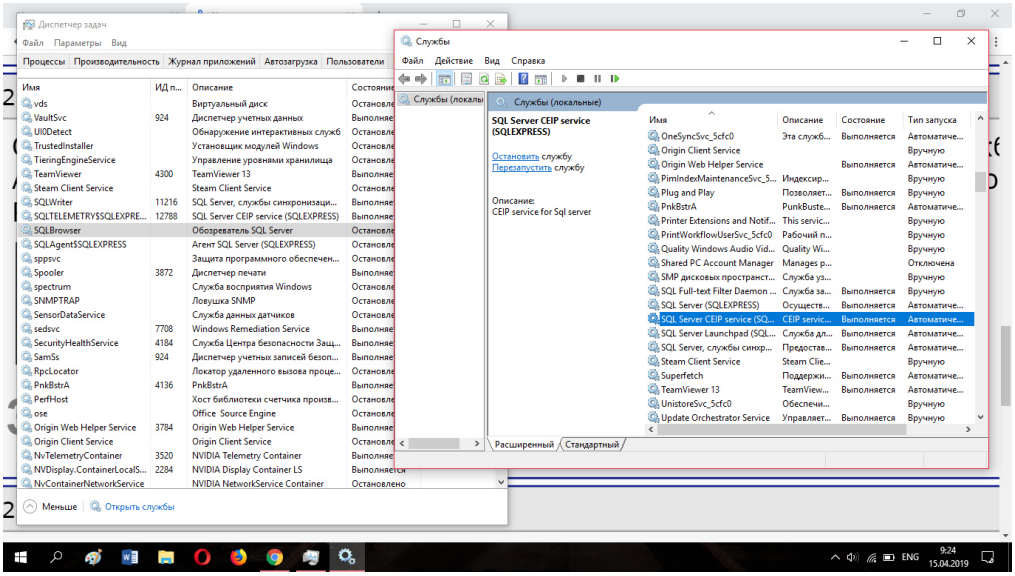
Жүйенің сервермен байланысын тексеру қажеттілігі туындайды. Осы жерде сервер типі мен қосылыс түрі таңдалады.



Сурет 22 – сервермен қосылысты тексеру

Егерде қосылмаған жағдайда: тапсырмалар диспетчеріне кіріп төмендегі опцияларды қосу қажет:

Диспетчер задач > процессы > SQLBrowser > ПКМ > Открыть > Включить



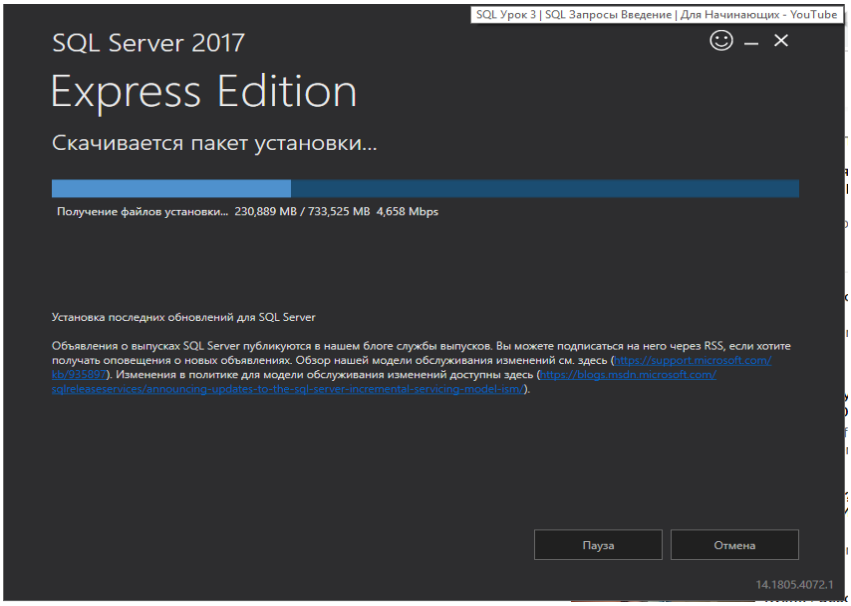
Сурет 23 – серверді қосу процесіндегі опциялар

SQL Server Express Microsoft SQL Server деректер қорын басқару жүйесінің ақылы, толық нұсқаларының көптеген мүмкіндіктерін ұсынады. Алайда, ол кейбір ірі масштабты өрістету үшін жарамсыз ететін техникалық шектеулерге ие [9].

MSDE-ден айырмашылығы, Express, егер Database Engine компоненті әдетте пайдаланушылар саны аз, жүктеме көп болса, параллельді жұмысты реттеп отыру мүмкіндігін қамтымайды. SQL Server Express деректер қорын басқару үшін бірнеше графикалық құралдарды қамтиды. Оларға жатады:

- SQL Server Management Studio;
- SQL Server Configuration Manager;
- SQL Server Surface Area Configuration tool;
- SQL Server Business Intelligence Development Studio.

Қарастырылып отырған жұмыста SQL Server Management Studio версиясы қолданылады(24-сурет).

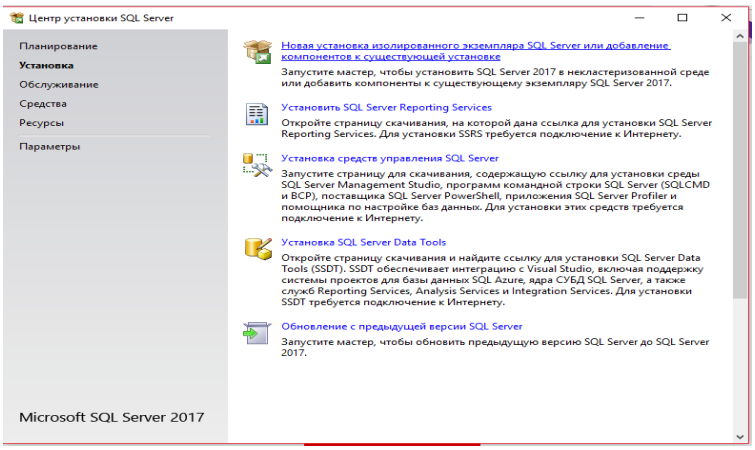


Сурет 24 - SQL express орнату пакеті

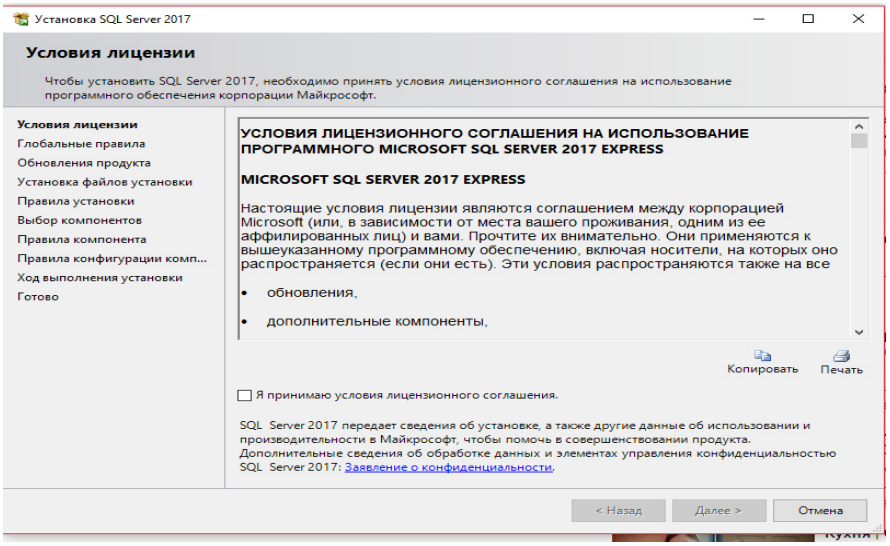
SQL express–ті орнату процесін сол процестердің үздіксіз жасалған скриншоттары арқылы көрсеткен түсініктірек болады.

Орнату үшін(25-34-сурет)**:**

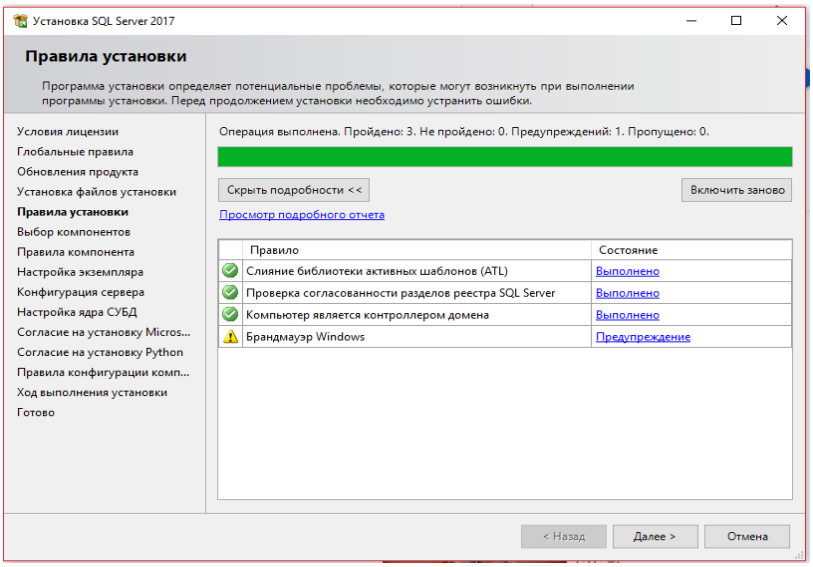
1-пунктті таңдаймыз



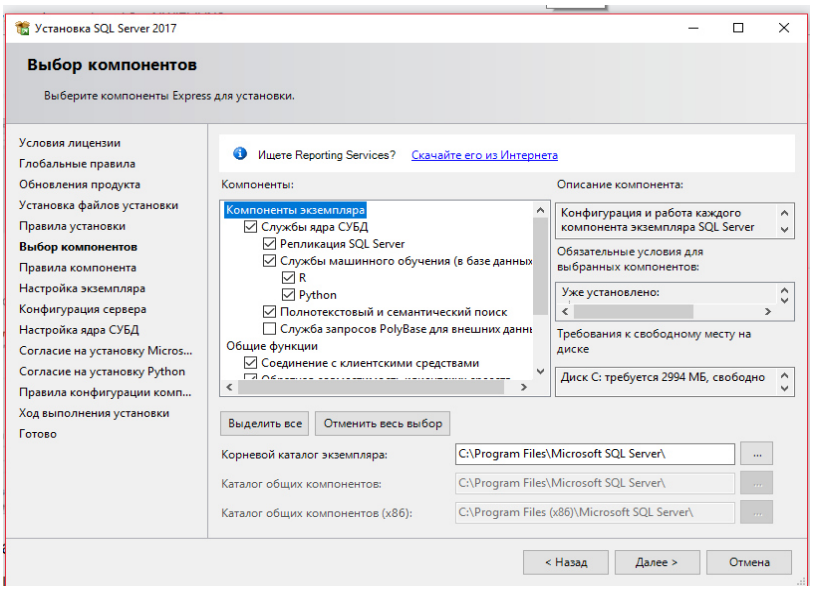
Сурет 25 – Орнату опциялары



Сурет 26 – Лицензия шартын анықтау

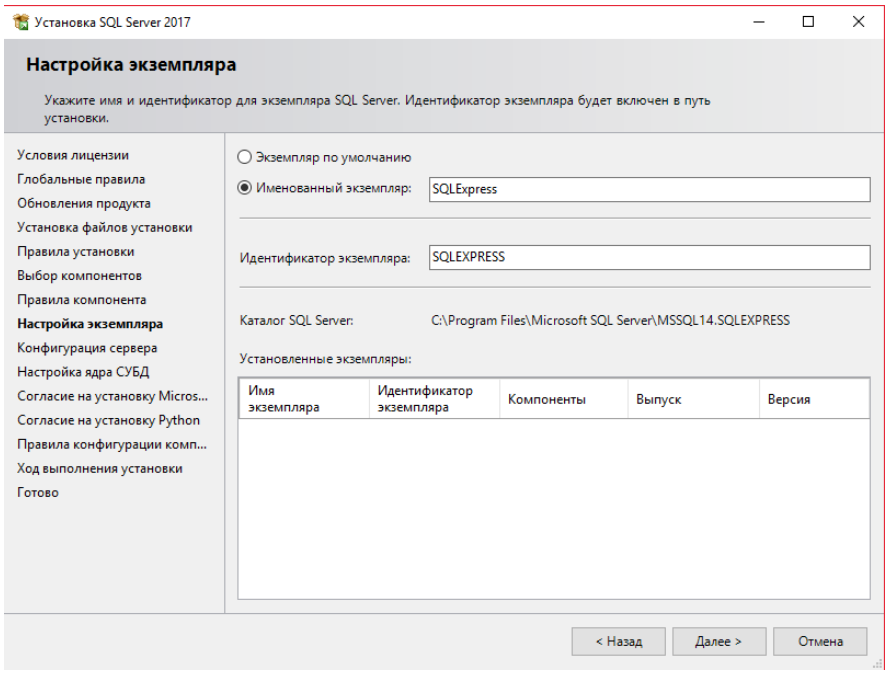


Сурет 27 – ортану ережелерін таңдау



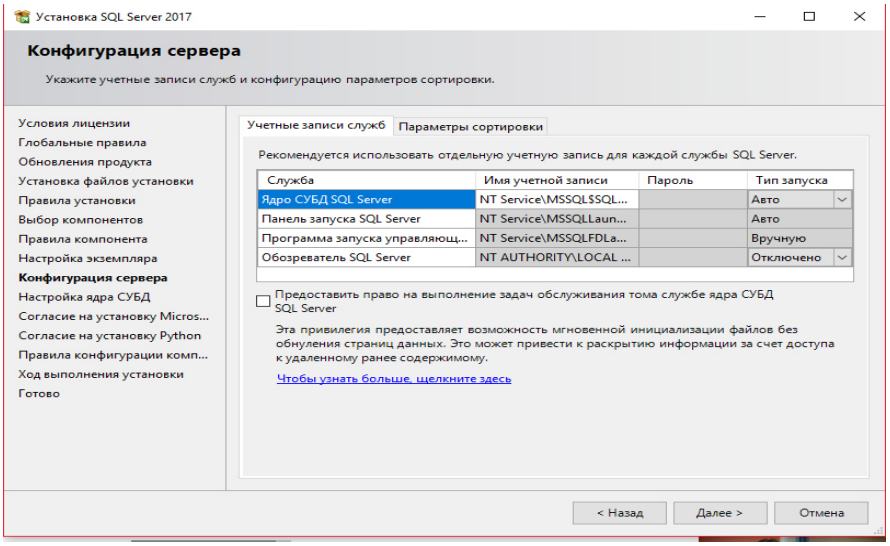
Сурет 28 – Орнатуға арналған Express компоненттері

SQL Server 2017 экземпляры үшін аты мен идентификаторын көрсету қажет. Экземпляр идентификаторы орнату жолында көрсетілетін болады.

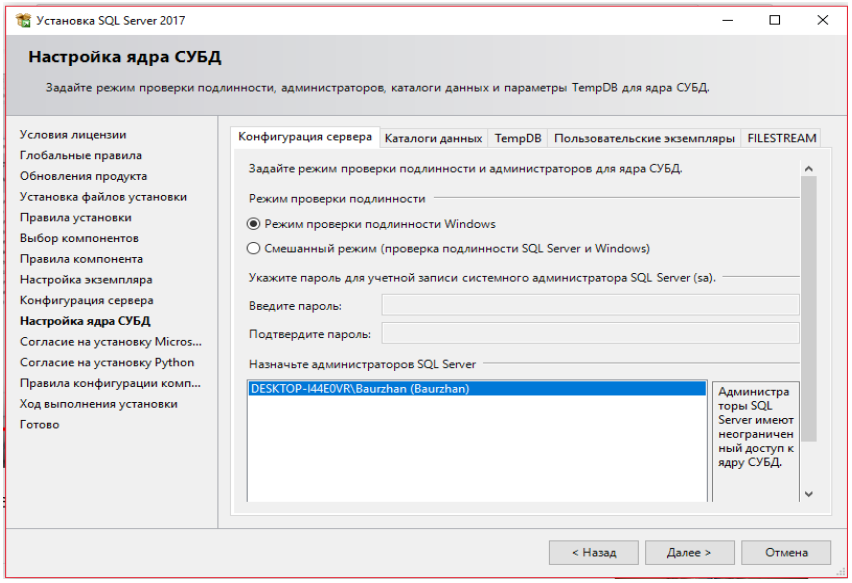


Сурет 29 – Экземплярды баптау

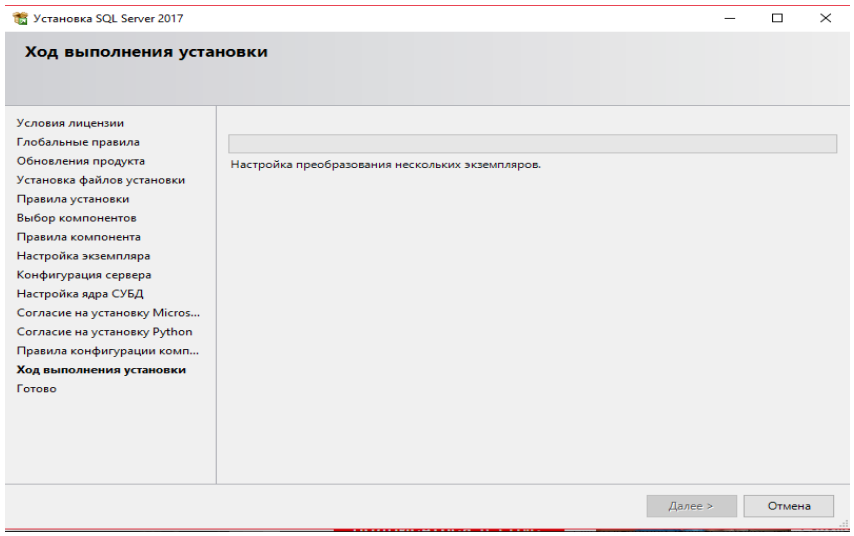
Әрі қарай сервер конфигурациясы бапталады. Ол жерде SQL Server-дің әрбір қызметі үшін жеке тіркеу жазбасын пайдалануға кеңес беріледі.



Сурет 30 – сервер конфигурациясын баптау

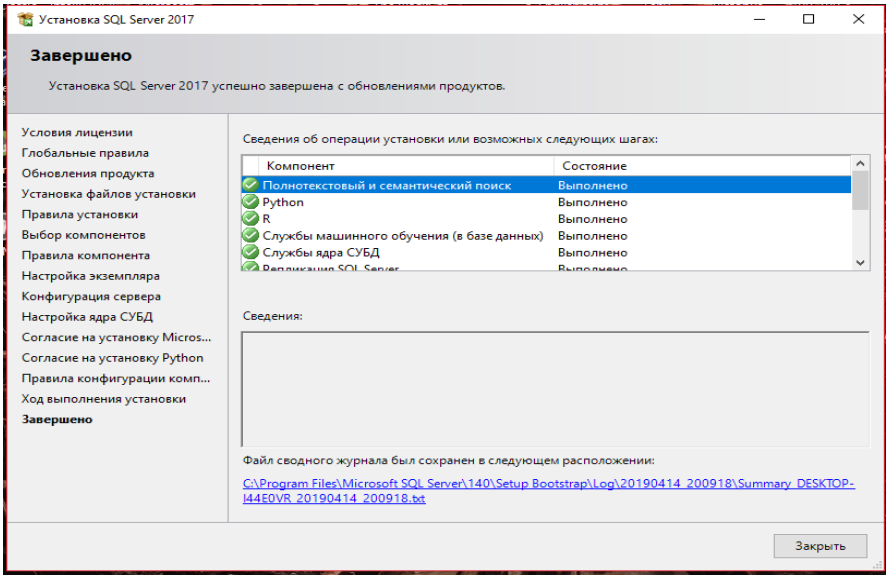


Сурет 31 – ДҚБЖ ядросын баптау

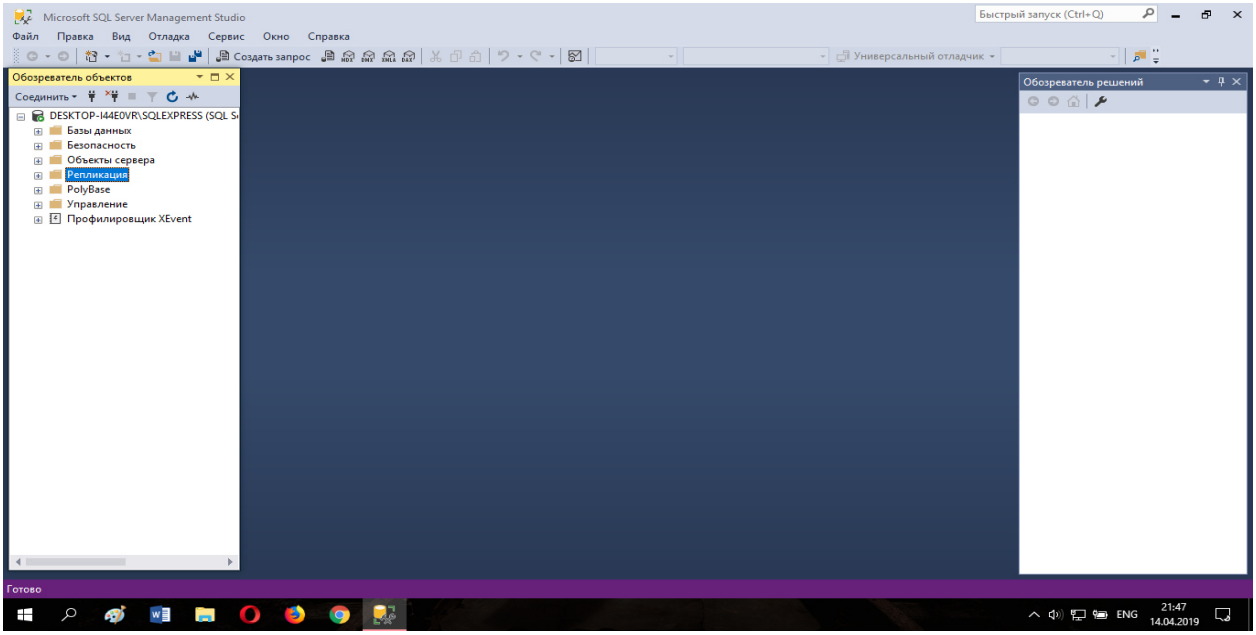


Сурет 32 – орнату барысын жалғастыру

Программа орнатылып болды деп есептесек, оның жарлықтар мен дистрибутивтері тиісті орнатылған программалар атауларының қатарында тұруы тиіс. Программаның толық орнатылып болғанына көз жеткізгеннен кейін оны жүктеуге болады [10].



Сурет 33 - SQL Server-ді орнату аяқталды



Сурет 34 – SQL Server Management қосылды

2.1Қауіп түрлері

Сала бойынша шабуылдардың танымалдығы Пилоттық жобалар барысында "SQL операторларын енгізу" және "ОС командаларын орындау" жиі кездеседі, мұндай PT AF шабуылдары жүйенің 80%-дан астамында тіркелген. Path Traversal анықталған шабуылдардың арасында танымалдығы бойынша екінші орынды алады.

SQL-кодты енгізу (ағылш. SQL injection) – еркін SQL-кодты сұрауға енгізуге негізделген деректер қорымен жұмыс істейтін сайттар мен бағдарламаларды бұзудың кең таралған тәсілдерінің бірі.

SQL енгізу қолданылатын ДҚБЖ түріне және енгізу шарттарына байланысты шабуылшыға деректер қорына ерікті сұраныс жасауға (мысалы, кез келген кестелердің мазмұнын оқу, деректерді жою, өзгерту немесе қосу), жергілікті файлдарды оқу және/немесе жазу және шабуыл жасалатын серверде ерікті командаларды орындау мүмкіндігін алуға мүмкіндік бере алады.

SQL енгізу типінің шабуылы SQL-сұраныстарда пайдаланылатын кіріс деректерін дұрыс өңделмеуінен болуы мүмкін.

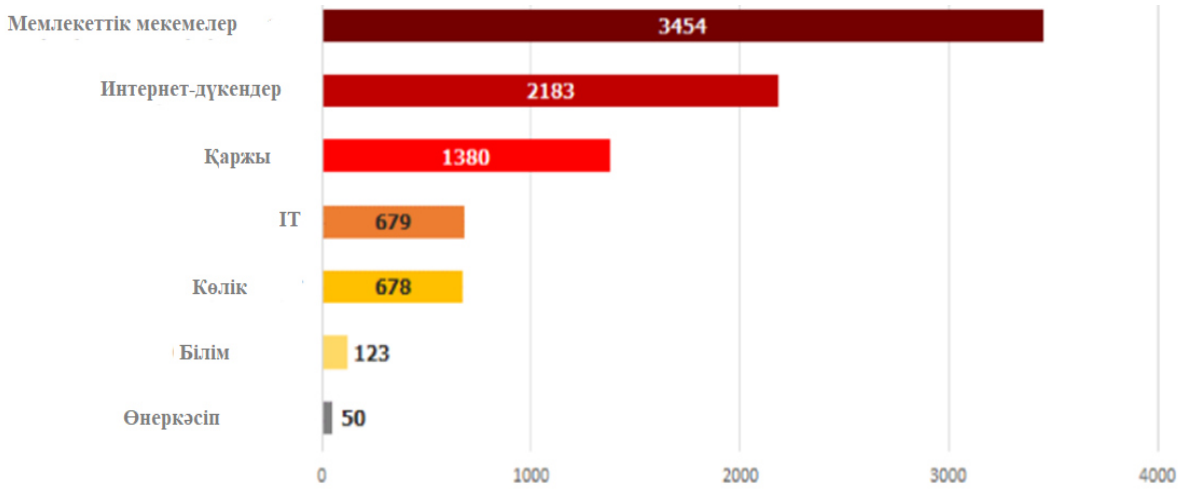
Деректер қорымен жұмыс істейтін қолданбалы бағдарламаларды әзірлеуші мұндай осалдықтар туралы білуі және SQL енгізуге қарсы іс-қимыл шараларын қабылдауы тиіс.

Әлбетте, бірінші кезекте зиянкестер орындау үшін ерекше жағдайларды талап етпейтін неғұрлым қарапайым шабуылдарды қолдануға тырысады. Негізінен, шабуылдарды анықтаудың төмен пайызы күрделіліктің жоғары деңгейін немесе оны іске асыру үшін арнайы шарттардың қажеттілігін, мысалы, веб-қосымшада файлдарды жүктеу функциясының болуын немесе пайдаланушылар тарапынан белгілі бір әрекеттерді жасауды куәландырады. Ең танымал шабуылдардың рейтингін жасау кезінде зерттеушілер мынадай нәтижеге қол жеткізген: мысалы, Acunetix, sqlmap(35-сурет) [11].

Сурет 35 – Ең танымал шабуылдардың рейтингі (веб-қосымшалар үлесі)

Бұл рейтингтегі шабуылдардың көпшілігі қауіпті осалдықтарды пайдаланады және бұл қаскүнемге жергілікті желі ресурстарына қол жеткізуге мүмкіндік береді.

PT AF жұмыс барысында тіркелген шабуыл түрлерінің арақатынасы және олардың саны зерттелетін жүйеге қатысты салаға байланысты өзгереді. Зиянкестер түрлі мақсаттарды көздейді, бұл ретте бұзушылардың біліктілік деңгейі мен техникалық мүмкіндіктері де ерекшеленеді. Келтірілген диаграммаларда бір жүйеге күндегі шабуылдардың орташа саны, сондай-ақ қолмен және автоматтандырылған сканерлеу үшін утилиталарды пайдалана отырып орындалатын шабуылдар санының арақатынасы берілген(36,37-сурет).



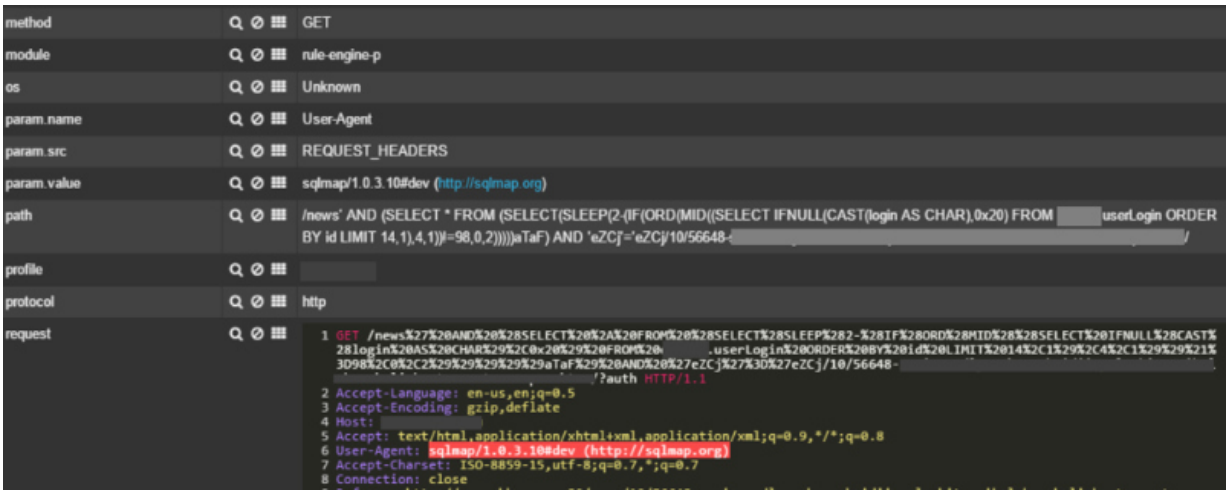
Сурет 36 - Бір жүйеге күніне шабуылдардың орташа саны

Сурет 37 – Қолмен орындалатын автоматтандырылған сканерлеу мен шабуылдардың арақатынасы

Мемлекеттік мекемелер мен интернет-дүкендерден басқа барлық салалар үшін шабуылдардың басым бөлігін осалдықтарды іздестіру үшін мамандандырылған БҚ көмегімен орындалатын шабуылдар құрайды. Автоматтандырылған сканерлеу шабуылдардың әр алуан түрлерін, мысалы, SQL, Path Traversal операторларын қорғауды дайын бағдарламалық құралдарын пайдалана отырып енгізу әрекеттерін қамтиды. Сканерлеу нәтижелерін зиянкестер осалдықтарды пайдалану және сезімтал ақпаратқа, жергілікті желі ресурстарына, аса маңызды жүйелерге қол жеткізгенге дейін

шабуыл векторын одан әрі дамыту үшін немесе пайдаланушыларға шабуыл жасау үшін пайдалануы мүмкін.

Төмендегі суретте sqlmap утилитасы арқылы автоматтандырылған сканерлеуді анықтауға мысал келтірілген. PT AF User-Agent-тегі HTTP тақырыбының қажетсіз құрамын және және SQL операторларының енгізілуін қамтитын сұранымды анықтайды(38-сурет) [11].



Сурет 38 – Автоматтандырылған сканерлеуді анықтау мысалы

Күніне ең көп шабуылдар саны – шамамен 3500 шабуыл, мемлекеттік мекемелерде пилоттық жобалар барысында тіркелген. Осалдықтарды автоматты түрде іздеу шабуылдардың жалпы санының 18% ғана құрайды. Интернет-дүкендер осы рейтингте екінші орында: күніне 2200-ге жуық шабуыл тіркелді, бұл ретте олардың барлығы автоматтандырылған сканерлеу құралдарын пайдаланбай жүргізілді.

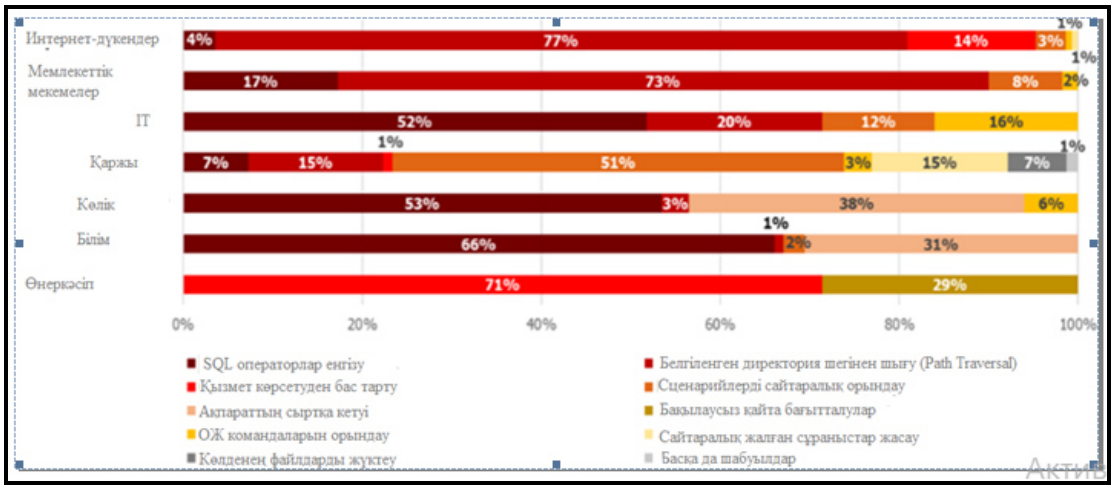
PT AF қаржы саласында күніне 1400-ге жуық шабуыл тіркелді, олардың арасында осалдықтарды автоматты түрде іздеу басым болды. Көлік ресурстары мен IT-компанияларға орташа есеппен күніне шамамен 680 шабуыл келеді, олардың басым бөлігі осалдықтарды автоматты түрде іздестіруді құрайды.

Білім беру саласы үшін күніне шабуылдардың орташа анықталған, ең көп шабуыл жасаған мезгіл ол ҰБТ немесе БҰКТ тапсыру кезі болған, ол кезде – күніне 20 000 астам шабуыл болған. Бұл ретте ең көп таралған шабуылдар осалдықтардың бар-жоғына сканерлеудің құрал-саймандық құралдарын пайдаланумен жүзеге асырылған. Оқушылар ақпараттық қауіпсіздік және қорғау механизмдерін айналып өту тәсілдері туралы базалық білімдерге ие бола отырып, жүйені сканерлеу үшін жалпы қол жетімді БҚ пайдалана алады. Сонымен, осы түрдегі шабуылдардың басым бөлігі АҚШ-тың тарапынан шыққаны түсіндіріледі: жария утилиттер немесе онлайн-сервистер АҚШ аумағында орналасқан прокси-серверлерді пайдаланған болуы мүмкін. Ақпараттық-талдау орталығына шабуыл жасаудың мақсаты емтихан нәтижелері мен емтихан материалдарына қол жеткізу болды. Мүмкін,

оқушылар емтихан алған ұпайларын осылай өзгерте алады деп ойлаған шығар.

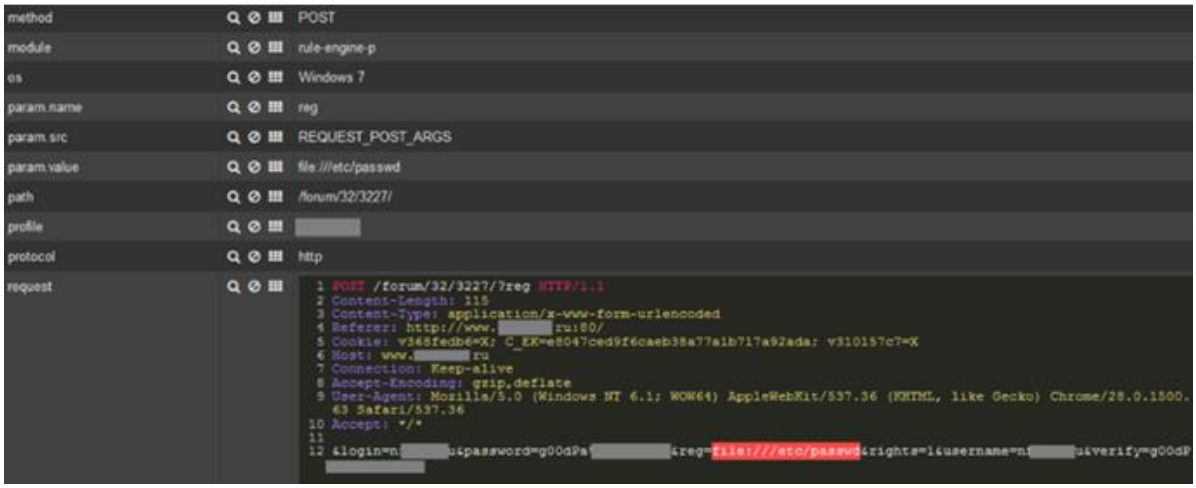
Өнеркәсіптік жүйелер үшін PT AF күніне 50-ге жуық шабуылдарды тіркеді, барлығы осалдықтарды автоматты түрде іздеу болып табылады және тек 1% қолмен жүргізілді.

Келесі диаграммада әрбір сала үшін зиянкестер жүзеге асыратын шабуылдар түрлерінің арақатынасы ұсынылған, бұл ретте есептерден осалдықтардың болуына автоматтандырылған сканерлеу шеңберінде жасалатын шабуылдар алынып тасталды, себебі олар нақты салалар үшін ерекше болып табылмайды(39-сурет) [11].



Сурет 39 – Қолмен орындалатын шабуыл түрлерінің арақатынасы

Мемлекеттік мекемелер үшін 70%-дан астамын Path Traversal шабуылдары құрады, олардың көмегімен зиянкестер файл жүйесінің ағымдағы каталогына, одан тыс жерлерге және сезімтал ақпаратты ұрлау мақсатында сервердегі файлдарға қол жеткізуге тырысты. Path Traversal шабуылын анықтау мысалы төменде көрсетілген. Қаскүнем сервер түпкі директориясына шығуға және /etc/passwd файлына кіруге ниет білдірді(40-сурет).



Сурет 40 – Path Traversal " шабуылын анықтау мысалы»

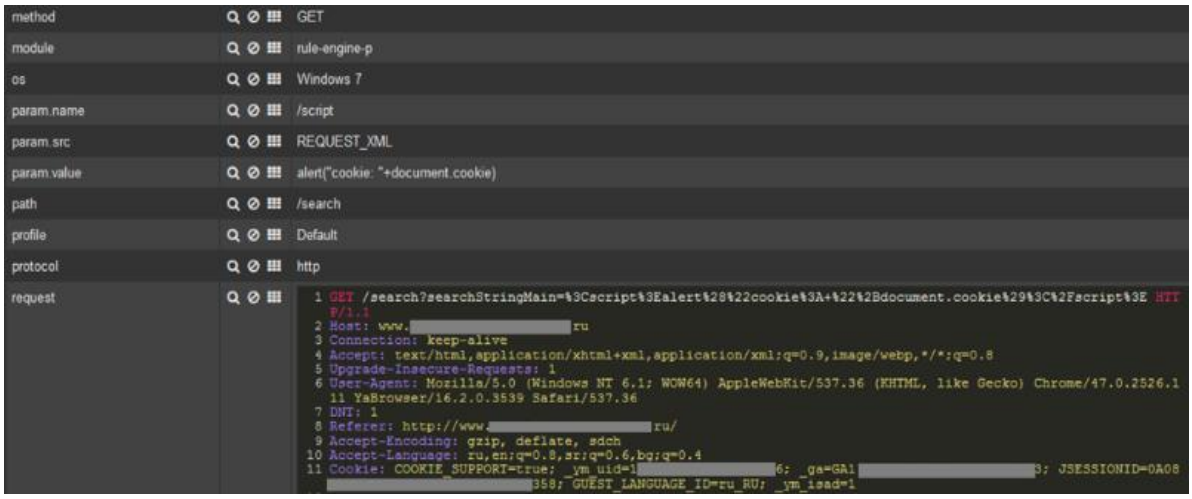
Шабуылдардың шамамен 17% SQL операторларын енгізу әрекеті болып табылады. Шағын бөлігін (8% - ға жуық) мемлекеттік көрсетілетін қызметтер порталдарын пайдаланушыларға бағытталған "сценарийлерді Интернетаралық орындау" шабуылдары құрайды. ОЖ командаларын зиянкестер 2% оқиғада орындауға тырысты.

Интернет-дүкендерге шабуыл жасаудың үштен бір бөлігі Path Traversal шабуылдарын құрады. Мемлекеттік қызметтерді ұсынатын порталдардағыдай зиянкестер файлдық жүйенің ағымдағы каталогынан тыс шығуға әрекет жасады. Елеулі бөлігі (14%) қызмет көрсетуден бас тартуға шабуылдарды құрайды. Интернет-дүкен үшін веб-бағдарламаның қолжетімділігін бұзу қаупі сыни болып табылады. Пайдаланушыларға жасалған шабуылдар ("сценарийлердің сайттағы орындалуы "және" сайттағы сұраныстарды қолдан жасау") жалпы көлемі 4%-ды құрайды. 4% жағдайда SQL операторларын енгізу де кездеседі.

Қаржы саласында 65%-ға жуық шабуылдарды жүйелерді пайдаланушыларға бағытталған "сценарийлерді Интернетаралық орындау" және "интернетаралық сұраныстарды қолдан жасау" шабуылдары құрайды [12].

Мұндай шабуылдар қаржы саласында кеңінен таралған және ерекше қауіп тудырады, өйткені Cookie мәндерін және пайдаланушылардың есептік деректерін (фишинг көмегімен) ұрлауға, сондай-ақ заңды пайдаланушылардың атынан әрекет жасауға мүмкіндік береді.

Суретте "сценарийлердің Сайтаралық орындалуы" шабуылын анықтау мысалы келтірілген. Қаскүнем осы шабуылға веб-қосымшаның осалдығын тексеру үшін Cookie мәнін экранға шығаруға тырысты(41-сурет).



Сурет 41 – «Сценарийлерді сайтаралық орындау» шабуылдарын анықтауға мысал

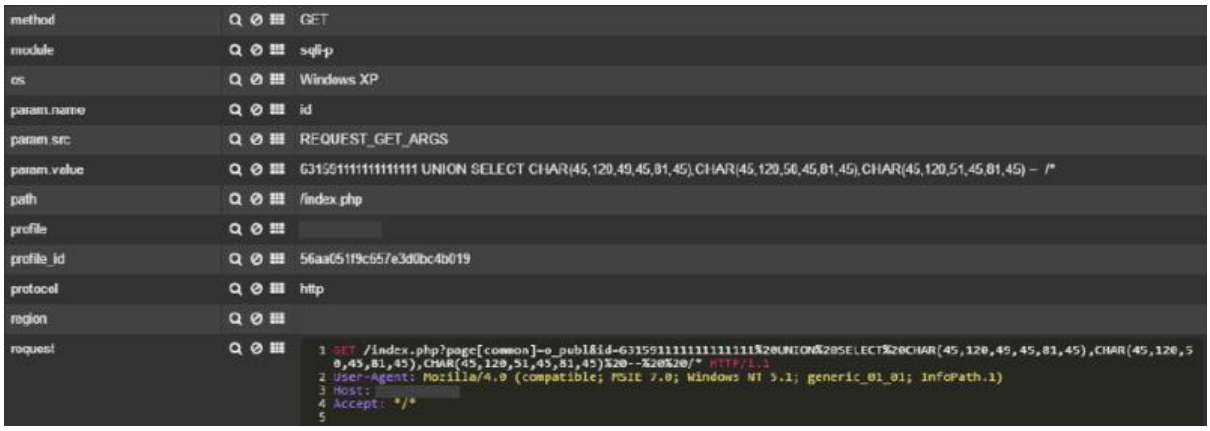
Зиянкестер Path Traversal шабуылының (жалпы санның 15%) және SQL операторларын енгізудің (жалпы санның 7%) көмегімен сезімтал ақпаратқа қол жеткізуге тырысты. "Еркін файлдарды жүктеу" шабуылдарының үлесі 7%-ды құрады. Мұндай шабуылдар ОЖ командаларын орындауға рұқсат алу үшін

жиі қолданылады, бұл ретте ОЖ командаларын тікелей орындау 3% жағдайда тіркелген. Жалпы, шабуылдардың сипаты мен күрделілігі зиянкестердің техникалық дайындығының басқа қарастырылатын салалармен салыстырғанда анағұрлым жоғары деңгейін білдіреді.

IT саласында тіркелген шабуылдардың жартысынан астамы SQL операторларын енгізу әрекеттері болып табылады. Path Traversal шабуылдары да бар (жалпы санының 20%). Бұдан басқа, 16% ОЖ командаларын орындау әрекеті болып табылады, ал IT-компаниялардың веб-қосымшаларына шабуылдардың 12% жүйе пайдаланушыларына бағытталған. Көлік компанияларының веб-қосымшалары үшін "SQL операторларын енгізу" шабуылдарының саны 50%-дан асады, шамамен 38% - ы ақпараттың жылыстауын және 6%-ы - ОЖ командаларының орындалуын құрайды [12].

Білім беру саласында қолмен орындалатын шабуылдардың шамамен 70%-ын "SQL операторларын енгізу" құрайды. Бұл шабуыл көбінесе қарапайым болып табылады, оны пайдаланушылардың жеке кабинеттеріне немесе деректер қорының мазмұнына қол жеткізу үшін пайдалануға болады. Шабуылдардың 30%-ға жуығы зиянкестерге сезімтал деректерді алуға немесе жүйе туралы қосымша ақпаратты білуге мүмкіндік беретін "ақпараттың жылыстауы" осалдығын пайдалануды білдіреді.

Суретте SQL операторларының енгізілуін анықтау мысалын көруге болады, қаскүнем осалдықты пайдалану мүмкіндігін тексеру үшін деректер қорына id –де GET-параметрінде өз сұранымын енгізген(42-сурет).



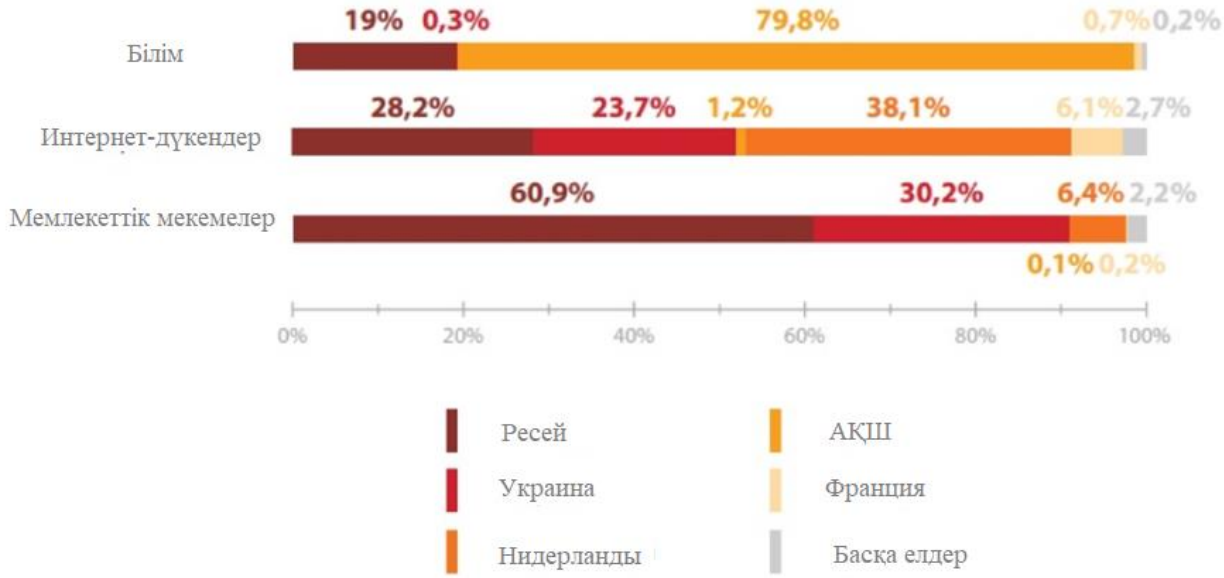
Сурет 42 – «SQL операторларын енгізу» шабуылын анықтау мысалы

Өнеркәсіптік кәсіпорындардың қосымшаларына шабуылдардың үштен екісі қызмет көрсетуден бас тартуға (DDoS) шабуылдарды құрады. Төменде суретте DDoS қоса, үш шабуыл тізбегін табу үлгісі көрсетілген. PT AF желіаралық экраны мұндай тізбектерді автоматты түрде, бірдей уақыт ішінде таратылған, бірақ бір шабуылдың бөліктері болып табылатын, оқиғалар арасындағы корреляцияларды анықтаудың арқасында құрады (43-сурет) [12].

Сурет 43 – DDoS-ты қоса алғанда, байланысты оқиғаларды анықтау мысалы

2.2 Шабуыл көздері

Шабуыл көздерін талдау пилоттық жобаларға қатысқан ресейлік жүйелерге қатысты ғана жүргізілген. Тіркелген шабуылдардың ең көп саны орыс тілінде сөйлейтін елдерден шығады, бірінші орында Ресей мен Украина тұр. Нидерланды мен АҚШ елдерінің аумағында прокси-серверлер қызметін ұсынатын провайдерлер саны көп болғандықтан, шабуылдар көзі осы елдерде жоғары пайызға ие болып отыр(44-сурет).



Сурет 44 – Шабуыл көздері болып табылатын елдер

2.2.1 Салалар бойынша шабуылдардың сыртқы көздері

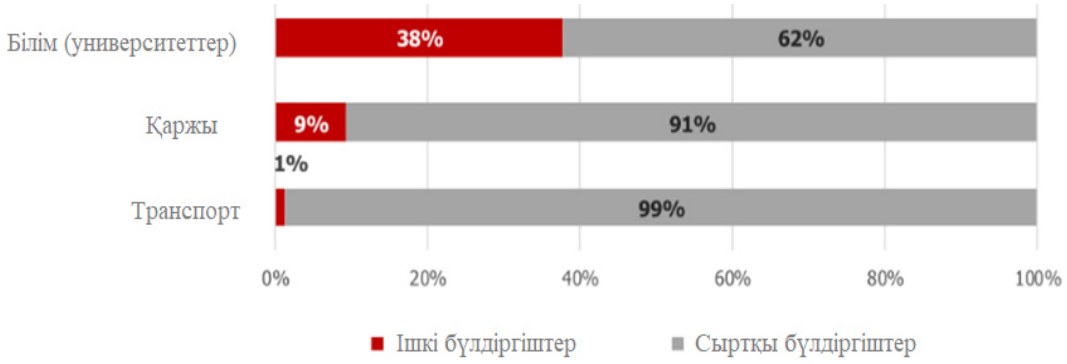
Ресей ұйымдарына сыртқы шабуылдардың көздері салаға байланысты ерекшеленеді. Мемлекеттік мекемелерге шабуылдардың басым бөлігі ресейлік IP-адрестерден жасалады, үштен бір бөлігі украиндық провайдерлерге тиесілі

IP-адрестерден жасалады, 6% жағдайда шабуыл көзі Нидерланды болып табылады.

Интернет-дүкендерге арналған шабуылдардың көзі шамамен тең үлеспен (жалпы санның төрттен бір бөлігі) Ресей мен Украина болып табылады. Шабуылдардың үштен бірінен астамы Нидерландының IP-адрестері арқылы өтеді.

Білім беру саласына шабуыл жасау үшін, жоғарыда көрсетілгендей, осалдықтардың болуына веб-қосымшаларды сканерлеу үшін көпшілік сервистер мен утилиттер кеңінен қолданылады. Шабуыл көзінің нақты IP-мекенжайын жасыру үшін мұндай БҚ негізінен АҚШ аумағында орналасқан серверлерді іске қосады. Шабуылдардың бесінші бөлігі ресейлік IP-адрестерден келеді.

Университеттердің веб-қосымшаларына шабуылдардың үштен бірінен астамының көзі ішкі зиянкестер болып табылады (орта есеппен білім беру саласы үшін бұл көрсеткіш 8%-ға тең). Бұл білім беру мекемесінің сымсыз желілеріне қол жеткізе алатын, сондай-ақ оқу аудиторияларында жергілікті желіге қол жеткізе алатын оқушылар болуы мүмкін(45-сурет).



Сурет 45 – Сыртқы және ішкі тәртіп бұзушылардың арақатынасы

Қаржы саласында ішкі тәртіп бұзушылардан шабуылдардың 10%-ға жуығы шығады. Сондай-ақ, тәртіп бұзушы бірқатар жағдайларда қорғаныс механизмдерін тестілеуді жүргізетін жүйенің әкімшісі болуы мүмкін деген нұсқа жоққа шығарылмайды [13].

2.3 Деректер қорына төнетін қауіптер түрлері, олардан қорғану әдістері

Қазіргі уақытта іс жүзінде барлық заманауи ұйымдар өз қызметінде деректер қорын пайдаланады. Деректер қоры (ДҚ) – бұл кез келген компания үшін ең маңызды және құнды актив. ДҚ-да өте маңызды немесе құпия ақпарат сақталуы мүмкін болғандықтан, оны қорғауға өте байыпты қарау қажет. ДҚБЖ мен деректер қорының жұмысындағы кез келген іркілістер апатты салдарға әкелуі мүмкін. Соңғы зерттеулердің нәтижелеріне сәйкес, деректер қорының бір жазбасының "құпиялылық-тұтастық-қолжетімділік" қасиеттерінің бірін бұзудан болған қаржылық залал $100-ден $240-ға дейін

құрайды. Сондықтан деректер қорының қауіпсіздігін қамтамасыз ету мәселесі өте өзекті болып табылады.

"ДҚ қорғау" деп кестелерде сақталатын ақпаратқа рұқсатсыз қол жеткізуді болдырмау әдісі түсініледі. Деректер қауіпсіздігін қамтамасыз ету (құпия деректерді қорғау) кезінде ең әлсіз орындардың бірі, әдетте, әртүрлі деңгейлерде оларға қол жетімділікті алатын адамдардың көп саны болып табылады. Яғни, деректер қорында сақталған ақпараттың қатері сырттан ғана емес, сонымен қатар заңды пайдаланушылар тарапынан да пайда болады. Ең типтік мысал, жүйелік әкімшінің жұмыстан шығар алдында деректер қорын жүктеу немесе лауазымдық міндеттеріне байланысты оған рұқсаты бар қызметкердің қорды ұрлауы болып табылады. Осылайша, ақпаратқа қол жеткізу арналарының қорғалу деңгейіне қарамастан, деректер қорының қауіпсіздігі корпоративтік талаптарға жауап беретініне сенімді болуға болмайды [14].

Деректер қорына шабуылдардың бірқатар технологиялары мен тәсілдері бар, олардың тиімділігі ол жұмыс істейтін деректер қоры мен сервердің конфигурациясына, АТ-инфрақұрылымы мен жалпы желі топологияларының қаншалықты дұрыс жобаланғанына және іске асырылғанына, адам факторы мен персоналдың адалдығына байланысты. Web-серверлерге және деректер қорының серверлеріне шабуылдар көбінесе сол мақсаттарды көздейді. Сондықтан деректер қорындағы ақпаратты қорғау жұмысы мен сәулетінде ұқсас ұстанымдары бар шешімдерді пайдалануға құрылады. Көптеген ДҚ қорғау құралдарының арасында негізгі және қосымша бөліктерді бөліп көрсетуге болады.

Негізгі ақпаратты қорғау құралдарына мыналарды жатқызады:

- парольдік қорғау;
- ДҚ кестелерінің өрістері мен жазбаларын қорғау;
- ДҚ объектілеріне қол жеткізу құқығын белгілеу;
- деректер мен бағдарламаларды шифрлау.

Қосымша қорғаныс құралдарына тікелей қорғаныс құралдарына жатқызуға болмайтын, бірақ деректердің қауіпсіздігіне тікелей әсер ететін мәліметтерді жатқызуға болады. Бұл:

- типтерге сәйкес деректер мәндерін бақылаудың кіріктірілген құралдары;
- енгізілген деректердің дұрыстығын арттыру;
- кесте байланыстарының тұтастығын қамтамасыз ету;
- желідегі ДҚ объектілерін бірлесіп пайдалануды ұйымдастыру.

Application Security компаниясы сарапшыларының пікірі бойынша, IT-қызметкерлері жиі елемейтін ДҚ-ның 10 негізгі қатері бар:

1) әдепкі, бос немесе әлсіз парольдер мен логин;
2) SQL-инъекция;
3) кеңейтілген баптаулар және топтық құқықтар;
4) ДҚ пайдаланылмайтын функцияларын активтендіру;
5) конфигурацияларды басқарудағы бұзушылық;

6) буфердің аса толуы;
7) артықшылықтар эскалациясы;
8) Dos-шабуылдар;
9) версиялары бойынша уақтылы жаңартылмаған;
10) тұрақты және мобильді құрылғыларда деректерді шифрлаудан бас тарту [14].

Деректер қорын қорғау және құпия ақпараттың қауіпсіздігін қамтамасыз ету үшін көптеген бағдарламалық шешімдер бар:

- FortiDB құралы;
- SafeNet Datasecure Материалдары;
- McAfee Database Security;
- Secret Disk Server NG құралы;
- крипто ДҚ: деректер қорын қорғау (Oracle);
- Datasecure және басқалар.

ДҚ қорғау құралдарының арсеналын жүйелі түрде қолданудан басқа әкімшілік және рәсімдік шараларды, атап айтқанда пайдаланушылардың парольдерін тұрақты түрде өзгерту, ақпаратты жеке тасымалдаушыларға қол жеткізуді болдырмау және т. б. қолдану қажет.

Осылайша, ақпараттық активтер кез келген ұйымның бизнесінің негізін құрайды, ал деректер қоры құрылымдалған ақпаратты сақтауға арналған басым құрал болып табылады. Аса маңызды деректерді ұрлаудың өсіп келе жатқан ауқымы деректер қорын қорғау қажеттілігін барынша өзекті етеді. Әсіресе маңызды ішкі зиянкестерден қорғау жүйесін құру болып табылады. Деректер қорымен жұмыс істейтін пайдаланушылардың іс-әрекеттерін бақылауды автоматтандыруда, сыртқы және ішкі қауіптерден қорғауда және деректер қорларының жұмыс істеу сенімділігін арттыруда маңызды рөл атқарады [14].

2.4 Сыртқы қауіп көзі. Инъекция типті шабуылдардың жұмыс сұлбасы

Деректер қорын қорғау шараларын қолданбас бұрын, алдымен деректер қорына төнетін қауіптерге талдау жасалып, нақты қандай қауіп түрінен қорғалу керектігі анықталу керек.

2.4.1 SQL-инъекция

Деректерді рұқсатсыз алу немесе қол жеткізу мақсатында зиянды кодтар енгізеді.

Шабуылдың мақсаты – веб-қосымшалардың деректер қорына бағытталған шабуыл.

Шабуылды жүзеге асыру кезінде қолданылатын осалдықтар – SQL-сұраныстарды сүзгіден өткізудің жеткіліксіздігі(46-сурет).

Сурет 46 – SQL шабуылды жүзеге асыру сұлбасы

Шабуылды жүзеге асыру кезінде қолданылатын программалар – Деректер қорлары осалдықтарының сканерлерін (SQLMAP, Automated Vulnerability Detection System (AVDS), Shadow Database Scanner, Acunetix және т.б.) және SQL программалау тілін білу маңызды [15].

Шабуыл объектісі – SQL-сервер.

Сипаттамасы – деректер қорына SQL-сұраныстар параметрлері өзгеретін шабуыл. Нәтижесінде сұрау мүлдем өзгеше мағынаға ие болады және кіріс деректерін сүзу жеткіліксіз болған жағдайда ақпаратты шығару ғана емес, деректерді өзгерту/жою да мүмкін. Шабуылдың мұндай түрін командалық жолдың параметрлерін (бұл жағдайда-URL айнымалылары) тиісті тексерусіз деректер қорына SQL-сұрауларды құру үшін пайдаланатын веб-сайттардың мысалында көруге болады.

Нәтижесі – SQL-инъекция шабуылының салдары деректер қорында сақталатын ақпаратқа (логиндер, парольдер, құпия ақпарат және т.б.) рұқсат етілмеген қол жеткізуге әкеп соғады.

Қауіп көзі – сыртқы болып табылады және шабуылды жүзеге асыру кезінде қолданылатын осалдық - PHP кодының кіріс параметрлерін тексеру жеткіліксіз.

Қорғау шарасы:

1) қатарлық параметрлерді сүзгіден өткізу;

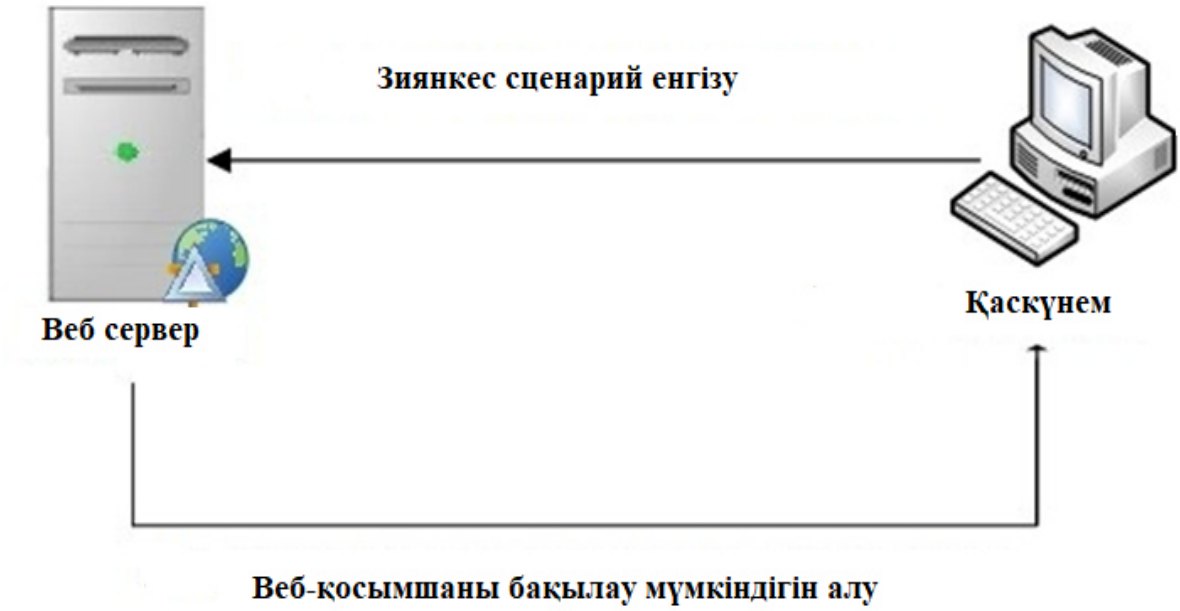
2) кіріс параметрлерін кесіп тастау (енгізілетін символдар санын шектеу);

3) SQL-инъекциядан қорғау жабдықтарын және Web Application Firewall (WAF) жабдығын қолдану.

2.4.2 PHP-инъекция

Шабуылдың мақсаты – Шабуыл бөтен (зиянды) PHP-кодын кейіннен бұзу үшін веб-қосымшаға енгізу болып табылады.

Қауіп көзі – сыртқы. Шабуылды жүзеге асыру кезінде қолданылатын осалдық - PHP кодының кіріс параметрлерін тексеру жеткіліксіз(47-сурет).



Сурет 47 – Шабуылды жүзеге асыру сұлбасы

Шабуылды жүзге асыру кезінде қолданылатын программалар – PHP программалау тілі. Шабуыл объектісі – Веб-қосымша.

Сипаттамасы – PHP жұмыс істейтін веб-бағдарламаларды бұзу тәсілдерінің бірі. Еркін командаларды өткізу мақсатында сайттың серверлік жағында веб-қосымшаның кодына арнайы қалыптасқан зиянды сценарийді енгізу болып табылады.

Нәтижесі – Инъекция сәтті болған жағдайда шабуылдаушы потенциалды қауіпті PHP-кодын орындай алады және веб-қосымшаны бақылауға алады [15].

Қорғау шарасы:

1 "Module" айнымалысын бөгде таңбаларға және рұқсат етілген мәндерге тексеру;

2 SQL-инъекциялардан қорғау құралдарын және Web Application Firewall-ды (WAF) пайдалану.

2.4.3 Сайтаралық скриптинг (XSS)

Шабуыл мақсаты – XSS шабуылы веб-қосымшамен берілетін зиянды код бетін (ол осы бетті ашқан кезде пайдаланушының компьютерінде Орындалатын болады) енгізуде және осы кодтың қаскүнемнің веб-серверімен өзара әрекеттесуінде жасайды.

Қауіп көзі – сыртқы. Шабуылды жүзе асыру кезінде қолданылатын осалдық – Бұл XSS қатері сервердің және Клиент жағында скрипті тілдердің осалдығына байланысты, негізінен HTML және JavaScript-ке (сонымен қатар VBScript, ActiveX, HTML және Flash) қатысты(48-сурет).

Сурет 48 – Жүзеге асыру сценарийі

Шабуылды жүзеге асыру кезінде қолданылатын программалар – Веб-қосымшалар осалдығы сканерлері (Acunetix, Cenzic Hailstorm Enterprise Application Risk Controller, HP WebInspect, IBM Security AppScan standart және т.б.).

2.4.4 CSS белгілеу тілін білу

Шабуыл объектісі – Веб-қосымша. Сипаттамасы – XSS шабуылы пайдаланушының авторизациялық деректерін алу үшін зиянды кодты енгізу болып табылады (әкімші сессиясының сәйкестендіргіші немесе төлем құжаттарының нөмірі). Зиянды код веб-сервердегі осалдық арқылы да, пайдаланушының компьютеріндегі осалдық арқылы да бетке енгізілуі мүмкін. Кейде желі аралық скриптинг DoS-шабуыл жасау үшін қолданылады.

Нәтижесі – Қаскүнем клиент жағында веб-қосымшаның скрипттеріне олардың орындалуын өзгертіп әсер етеді. Нәтижесінде бетке зиянды скрипт қосылады, ол бетті жүктеу кезінде немесе пайдаланушы деректерін рұқсатсыз алу мақсатында белгілі бір оқиға кезінде әрбір рет орындалатын болады [15].

Қорғау шарасы

Сервер жағында:

1) браузерде көрсетер алдында HTML-символдарды, JavaScript, CSS және URL кодтау. Кіріс параметрлерін сүзу үшін келесі функцияларды пайдалануға болады: filter_sanitize_encoded (URL кодтауы үшін), htmlentities (HTML сүзгісі үшін);

2) кіріс деректерін кодтау. Мысалы, мына кітапханаларжың көмегімен OWASP Encoding Project, HTML Purifier, htmLawed, Anti-XSS Class;

3) код қауіпсіздігін тұрақты қолмен және автоматтандырылған талдау және енуді тестілеу. Ол үшін мына құралдар қолданылады: Nessus, Nikto Web Scanner және OWASP Zed Attack Proxy;

4) әр web-бетте (мысалы, ISO-8859-1 немесе UTF-8) қандай да бір пайдаланушы өрістеріне дейін кодтауды көрсету;

5) доменді шектеу және қабылданатын cookies жолдарын, HttpOnly параметрін орнату арқылы жүзеге асырылатын cookies қауіпсіздігін қамтамасыз ету, SSL пайдалану;

6) JS, CSS, суреттер сияқты түрлі деректерді жүктеуге болатын қажетті көздер енгізілетін тізімді қоюға мүмкіндік беретін Content Security Policy тақырыбын пайдалану.

Клиент жағында:

1) браузерді соңғы нұсқаға тұрақты жаңарту;

2) пішін өрістерін тексеретін браузер үшін кеңейтімдерді орнату, URL, JavaScript және POST сұраулар, және скрипттер бар болса, оларды іске қосуды болдырмау үшін XSS сүзгілерін қолдану [16].

2.5 Деректер қорын қорғау құралдары

Деректер қорын қорғау құралдары деректер қорын және олар пайдаланатын деректер қорын басқару жүйелерін (ДҚБЖ) ақпараттық қауіпсіздік қатерінен қорғауға арналған. Деректер қорының ақпараттық қауіпсіздігінің негізгі қатерлеріне:

- деректерді бұрмалау, жою немесе ұрлау мақсатында адамдардың қасақана, деструктивті әрекеттері;
- сыртқы көздерден түсетін ақпаратты беру арналарында бұрмалау;
- дерекқордың жұмыс істеуіндегі іркілістер мен істен шығулар, құрамы мен конфигурациясының өзгеруі;
- қандай да бір себеппен белгіленген қауіпсіздік саясатын бұзатын немесе дұрыс емес қауіпсіздік әдістерін қолданатын жүйені пайдалану процесінде пайдаланушылардың, әкімшілік және қызмет көрсетуші персоналдың қателіктері мен санкцияланбаған әрекеттері;
- ДҚБЖ-да артықшылықтарды арттыруға бағытталған авторландырылған пайдаланушылар тарапынан шабуылдар;
- бағдарламалық және аппараттық қамтамасыз етудегі қателерге және оларды дұрыс теңшеуге және деректер қорының конфигурациясын күйге келтіруге байланысты туындайтын қауіптер;
- базаны жобалау, әзірлеу және іске асыру кезіндегі қателер, соның ішінде жүйелік ;
- ДББЖ осалдықтарының болуы.

Деректер базаларында сақталатын ақпарат қатерлері сырттан ғана емес, әкімшілік және қызмет көрсетуші персоналды қоса алғанда, заңды пайдаланушылар тарапынан да пайда болады. SQL тілі – деректерді анықтау және манипуляциялау құралы болып табылады.

- деректер базасын қорғаудың негізгі құралдары;
- деректер қорының желіаралық экрандары (Database Firewall);
- ДҚБЖ деректер қорының белсенділік мониторингі құралдары (Database Activity Monitoring, DAM) [16].

2.6 Деректер қорларының желіаралық экрандары (Database Firewall)

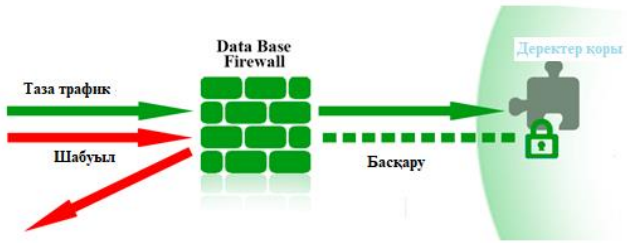
Деректер қорының желіаралық экрандары (Database Firewall) деректер қоры серверлерін жіберілген шабуылдардан және рұқсатсыз ауытқушылықтан қорғауды қамтамасыз етеді. Келесі негізгі функцияларды қамтиды:

- SQL-трафикті және SQL-сұраныстарды талдау, деректер қорының белсенділік мониторингі;

- SQL-шабуылдарды және дұрыс емес SQL-сұрауларды анықтау (SQL-кодты грамматикалық талдау "қара" және "АҚ" тізімімен SQL-сөйлемдер) және ауытқушылық мінез-құлық (мінез-құлық талдауы);

- анықталған SQL-шабуылдарды және аномальді рұқсат етілмеген сұраныстарды бұғаттау, SQL-сұраныстарды түзету.

Қосымша Database Firewall пайдаланушылардың іс-әрекеттерін бақылау және аудит, пайдаланушылардың қол жеткізу құқықтарын Бақылау, деректер базасына рұқсатсыз қол жеткізуден қорғау және деректер қорында осалдықтардың болуын бағалау функцияларын орындай алады(49-сурет).



Сурет 49 – Деректер қорына шабуылдан қорғауда желіаралық экранның орналасуы

2.7 ДҚБЖ деректер қорының белсенділік мониторингі құралдары (Database Activity Monitoring, DAM)

ДҚБЖ деректер қорының белсенді мониторинг құралдары (Database Activity Monitoring, DAM) нақты уақыт режимінде деректер қорына жүгінулер мониторингін жүргізеді, күдікті операцияларды анықтайды, ақпараттың ықтимал жылыстауы фактілерін анықтайды және деректер қорын қорғау сенімділігін арттырады. Келесі негізгі функцияларды орындайды:

- өтініштерді, сеанстарды және деректер қорына сұраныстарды бақылау, оларды талдау, әртүрлі өлшемдерге сәйкес жағымсыз және ықтимал қауіпті өтініштерді анықтау және оқшаулау;

- DML, DDL және DCL белсенділігін, оқуға арналған ақпаратты (select таңдауларын), сақталатын процедуралардағы, триггердердегі және басқа да деректер қорының объектілеріндегі өзгерістерді, сондай-ақ SQL қателерді, пайдаланушыларды авторлау әрекеттері мен ақпаратын қоса алғанда, деректер қорының барлық белсенділігін қадағалау;

- қарапайым пайдаланушылардың, сондай-ақ артықшылықты пайдаланушылардың және деректер қорының серверіне рұқсаты бар әкімшілердің өтініштерін, іс-әрекеттері мен операцияларын бақылау, мониторинг (аудит), оқыс оқиғаларды тексеру үшін аудитті талдау;

- ақпараттың ағуын болдырмау үшін дерекқор жауабын бақылау;

- ДҚБЖ жұмыс істеуіндегі аномалияларды бақылау және анықтау;

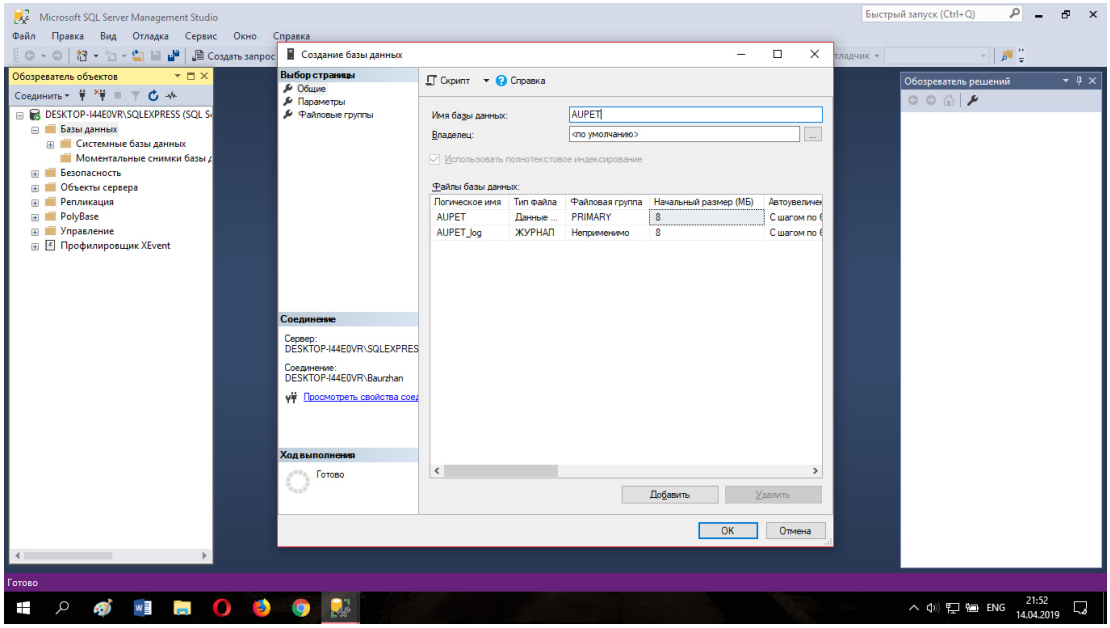
- деректер қорының өзгерістерін бақылау және басқару.

Қосымша Database Firewall пайдаланушылардың құқықтарын бақылау және басқару, деректер қорының осалдығын анықтау және жою функцияларын орындай алады [17].

3 Деректер қорын құру және қорғау

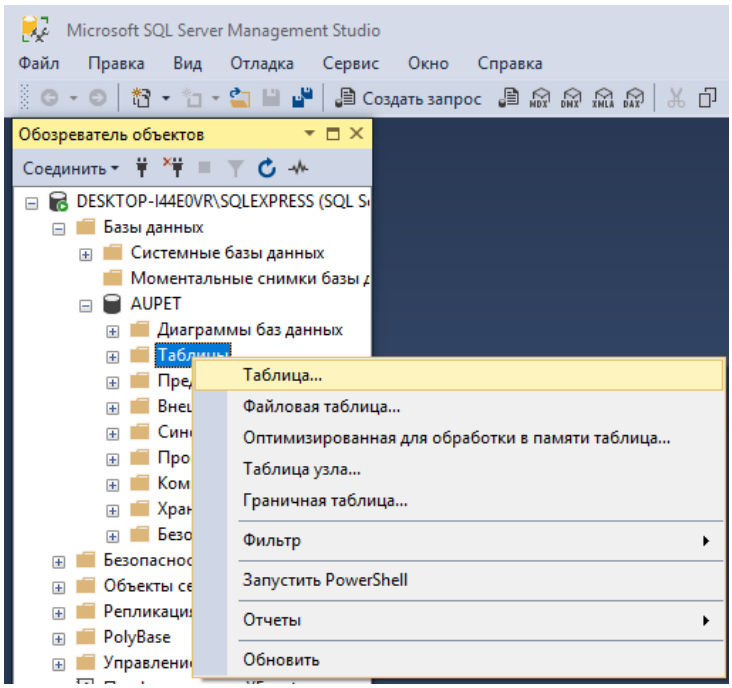
3.1 Деректер қорын құру

Деректер қорын жүзеге асыру үшін тұжырымдамалық модельді жобалау және оны таңдалған ДҚБЖ-да іске асыру қажет. Дайын логикалық модельді іске асыру процесі 50-суретте көрсетілген.



Сурет 50 – дайын логикалық модельді жүзеге асыру

Кестелерді жасау: Кесте құру үшін Деректер қоры→ Кесте опциясы таңдалады(51-сурет).

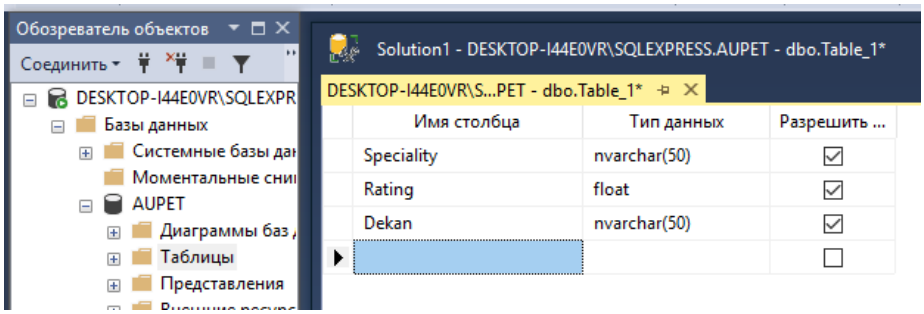


Сурет 51 – Бастапқы кестені құру процедурасы

Кесте құрастырушысы: Microsoft SQL Server Management Studio ортасында негізгі кесте құрылады. Кестенің атауы (3.1-сурет) және сол атау бойынша құрылатын кестеде қамтылатын деректер сипаттамасы беріледі (52-сурет) [18].

Кесте 3.1 – Негізгі кестелерге сипаттама

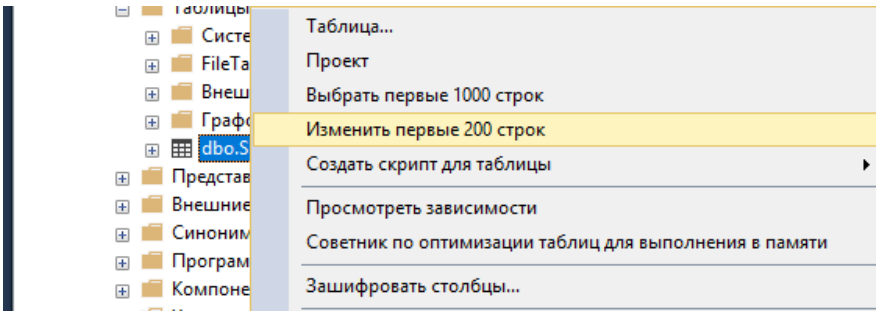
Кесте атауы	**Сипаттама**
Schudle	Кестелер бұтағындағы түпкі кесте - Teachers - Special - Lessons - Students
Teachers	Оқытушылар туралы мәліметтер сақталады. - Surname - Name - Speciality - Address
Special	Мамандықтар туралы деректер сақталады: - Speciality (мамандықтар) - Rating (мамандық рейтингі) - Dekan (мамандық қарасты деканат басшылары
Lessons	Мамандық бойынша оқылатын пәндер туралы мәліметтер сақталады.
Students	Студенттер туралы мәліметтер сақталады: - Name - Surname - Groups - NumberPhone - Address



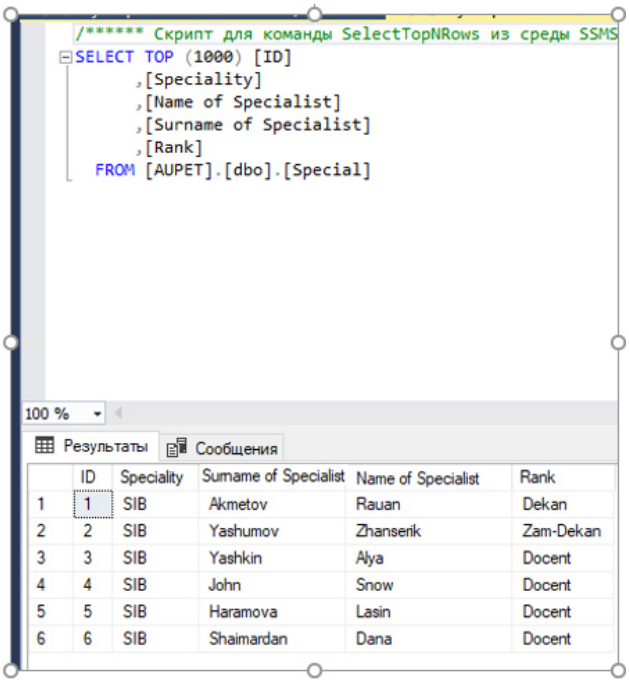
Сурет 52 – кестедегі ішкі салымдар

Кесте деректерін енгізу.

Жаңа жазбаларды қосу және MS SQL Server деректер қорының кестесіне өзгерістерді қарапайым жағдайда жасауға болады. SQL Server Management Studio бағдарламасында Нысандар шолғышында қажетті кестені таңдап, мәтінмәндік мәзірде бірінші 200 жолды өңдеу бойынша басу керек(53,54-сурет).

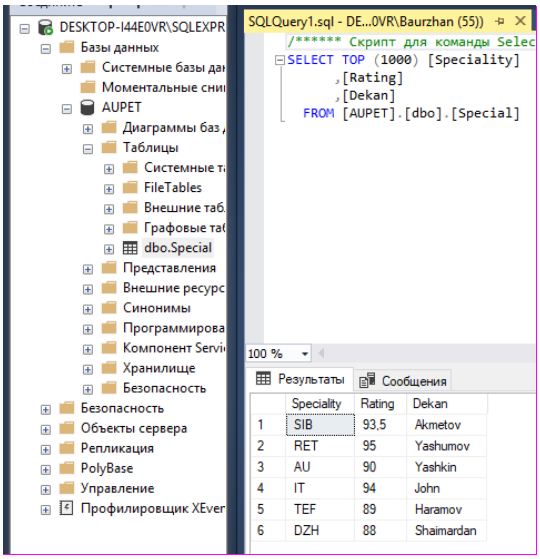


Сурет 53 – Қарап шығу/өңдеу үшін жолдар санын баптау



Сурет 54 – Мамандық және сол мамандыққа жауаптыларды бекіту кестесі

Мамандықтың рейтингі
Кестедегі деректерді қалай көруге болады(55,56-сурет):



Сурет 55 – мамандықтар, олардың рейтингілік көрсеткіштері кестесі

```
/****** Скрипт для команды Sele
SELECT TOP (1000) [Speciality]
      ,[Rating]
      ,[Dekan]
  FROM [AUPET].[dbo].[Special]
  WHERE Speciality = 'SIB'
```

00 %

Результаты | Сообщения

	Speciality	Rating	Dekan
1	SIB	93,5	Akmetov

Сурет 56 – Деректер қорынан бір ғана мамандықты таңдау форматы

Бірнеше кестелерді жасау: Жаңа жазбаларды кестеге енгізуге болады және ол SQL-дің Insert ұсынысы бойынша жүзеге асырылады(57,58-сурет).

```
/****** Скрипт для команды SelectTopNRows
SELECT TOP (1000) [ID]
      ,[Surname]
      ,[Name]
      ,[Speciality]
      ,[Address]
  FROM [AUPET].[dbo].[Teachers]
```

100 %

Результаты | Сообщения

	ID	Surname	Name	Speciality	Address
1	1	Axrapov	Almat	SIB	Medey
2	2	Shaikulova	Aktoti	SIB	Bostandynsky
3	3	Jaranova	Larisa	SIB	Bostandynsky
4	4	Hairushin	Shokan	SIB	Medey
5	5	Polanov	Serik	SIB	Bostandynsky
6	6	Karimov	Galina	SIB	Medey
7	7	Xowuneky	Sultan	SIB	Bostandynsky
8	8	Armanov	Erlan	SIB	Medey

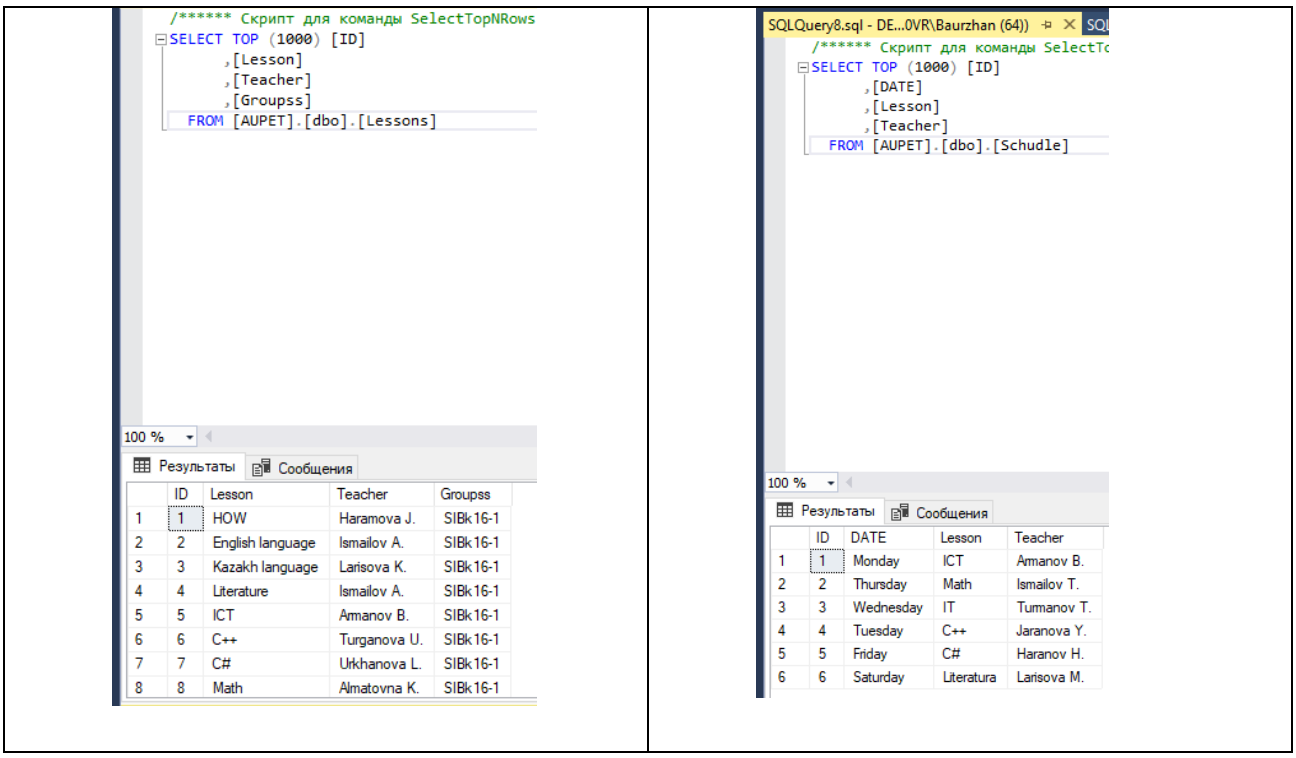
```
/****** Скрипт для команды SelectTopNRows из среды SSMS  ******
SELECT TOP (1000) [ID]
      ,[Name]
      ,[Surname]
      ,[Groups]
      ,[NumberPhone]
      ,[Address]
  FROM [AUPET].[dbo].[Students]
```

100 %

Результаты | Сообщения

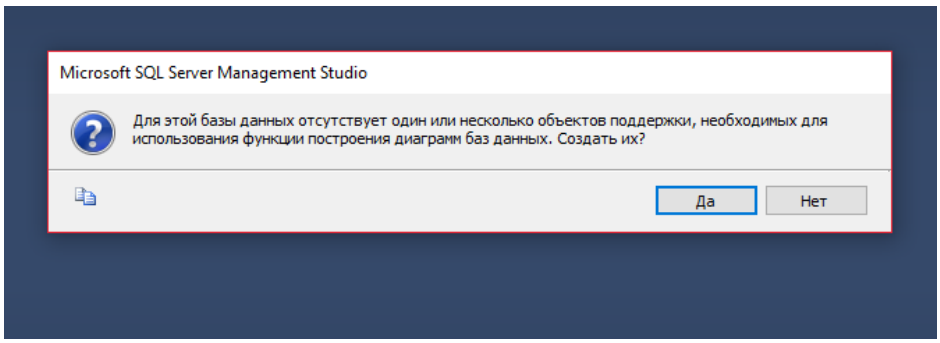
	ID	Name	Surname	Groups	NumberPhone	Address
1	1	Baurzhan	Yerlanov	SIBk16-1	8-707-575-55-04	Tatarka №44
2	10	Berik	Harmanov	SIBk16-1	8-875-898-74-74	Rostov №51
3	11	Kuatova	Zhuldyz	SIBk16-1	8-785-855-55-45	Raimbekov №54
4	12	Jaronov	Ismail	SIBk16-1	8-755-868-88-74	Kazibek Bi №16
5	13	Koreshov	Harion	SIBk16-1	8-998-788-88-88	Aiteke Bi №18
6	2	Abubakir	Mukhamed	SIBk16-1	8-999-999-88-88	Baitursynova №19
7	3	Eleusiz	Azamat	SIBk16-1	8-787-858-89-96	Baityrsynova №234
8	4	Shamshaev	Marsel	SIBk16-1	8-888-888-88-88	Timeryzova №1
9	5	Nolkin	Shokan	SIBk16-1	8-707-598-88-78	Timeryzova №25
10	6	Alikozha	Yermanov	SIBk16-1	8-574-587-88-77	Raimbekova №17
11	7	Arsenov	Larin	SIBk16-1	8-887-787-78-89	Golemov №13

Сурет 57 – мұғалімдер және студенттердің деректері толтырылған кестелер



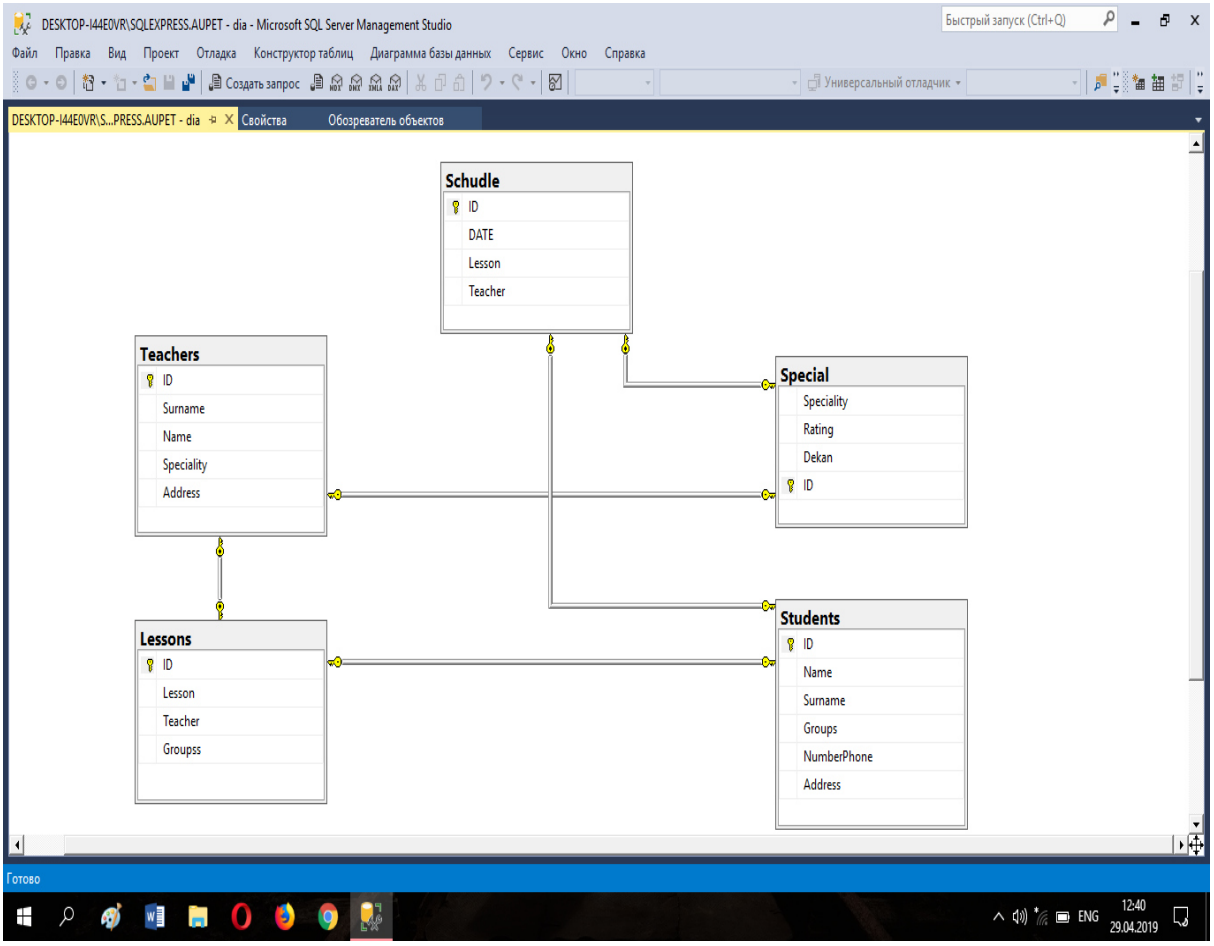
Сурет 58 – сабақ беретін мұғалімдер

Кесте диаграммасын құру(59-сурет):



Сурет 59 – Диаграмма құруға сұраныс

Мәліметтердің физикалық моделін іске асырамыз (60-сурет).



Сурет 60 - ДҚ диаграммасы

3.2 Әкімшілік бөлімге сипаттама

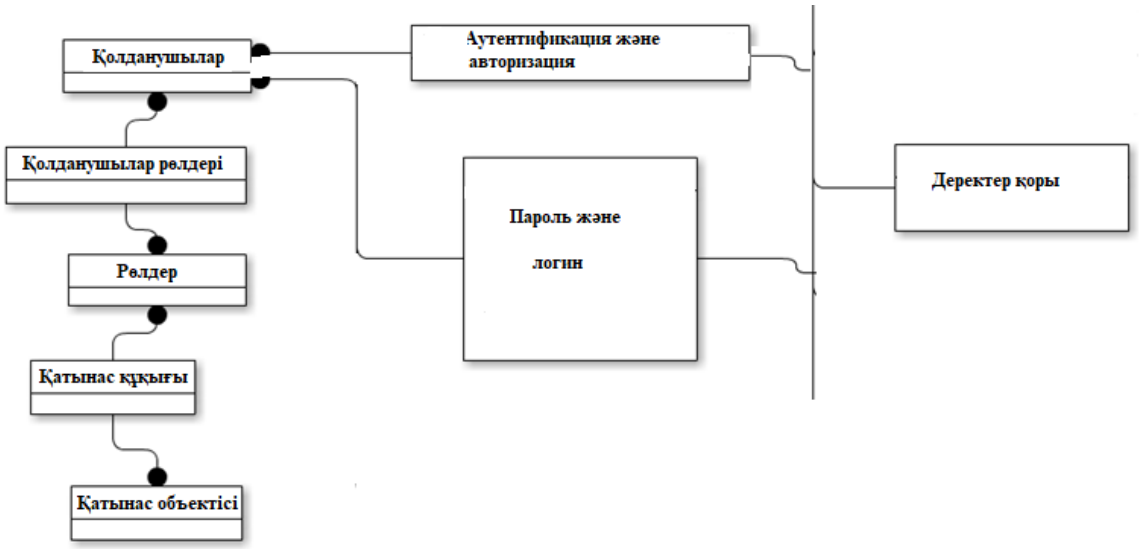
Әзірленетін жүйенің әкімшілік бөлімі қолданушылар құқығын бөлу, жүйені баптау және қауіпсіздік шараларын ұйымдастыру бөлімдерін қамтиды. Әкімшілік бөлім тек осы жүйенің әкімшісі үшін ғана қолжетімді, ол басты жүйенің көпшілікке арналған бөлігін басқару және ішкі жүйелерді басқару элементтерін қамтиды [19].

Негізгі жүйенің әкімшілік бөлігі келесі бөлімдерді басқаруға мүмкіндік береді

- пайдаланушылар - пайдаланушылардың есептік жазбаларын басқару;
- анықтамалықтар - анықтамалық ақпаратқа қол жеткізу;
- бағдарлама - мамандықтарды , оқытушыларды, студенттерді қосу, өзгерту, алып тастау.

3.2.1 Қатынас құқығын анықтау

Әкімші жүйе қолданушыларының қатынас құқығын анықтап береді, осылайша жүйеге енуді авторизациялау және аутентификациялау процесі жүзеге асырылады(61-сурет).



Сурет 61 – Қатынас құқығын анықтау құрылымы

Пайдаланушыларды аутентификациялаудың бірнеше балама бар. Кейбір жеке ақпаратты пайдаланушымен байланыстыру қажет болғандықтан, оның кіріс аты мен паролі MySQL деректер қорында сақталады және аутентификация үшін әр уақытта қолданылады. Егер пайдаланушылар өз аты мен паролін көрсете отырып, жүйеге кіру операциясын ұсыну қажет болса, бұл келесі компоненттердің қажеттілігін тудырады [20].

Пайдаланушыларды идентификациялау. Пайдаланушылардың жүйеде тіркелу мүмкіндігі болуы тиіс. Сонымен қатар, аты мен паролінің ұзындығы мен пішімін шектеу қажет. Құпия сөзді шифрланған түрде сақтау керек.

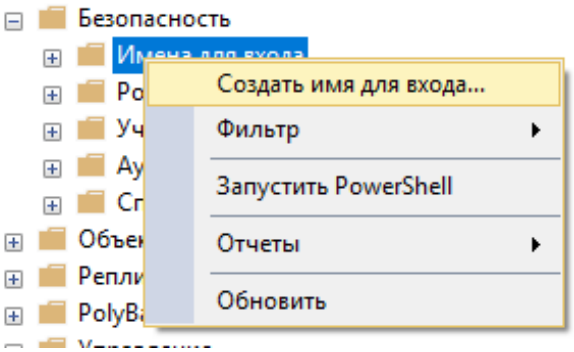
Пайдаланушылар тіркеу кезінде ұсынған мәліметтерді көрсете отырып, жүйеге кіруді ұсыну қажет.

Әкімші пайдаланушының жүйеге кіргенін тексеруге, сондай-ақ осы процедураны орындағандарға мәліметтер ұсынуға міндетті.

Пайдаланушылар кез келген уақытта өз құпия сөзін өзгертуге құқылы.

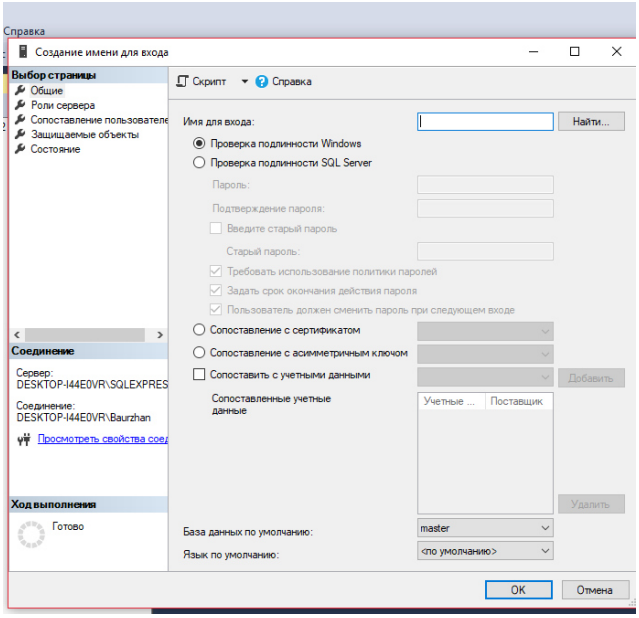
Админды құру үшін:

Қатынас құруды шектеу үшін кіру аттарын жасау керек. ДҚ салымында "қауіпсіздік" тармағын таңдап, онда "кіру аттары" тармағын таңдау қажет (62-сурет).

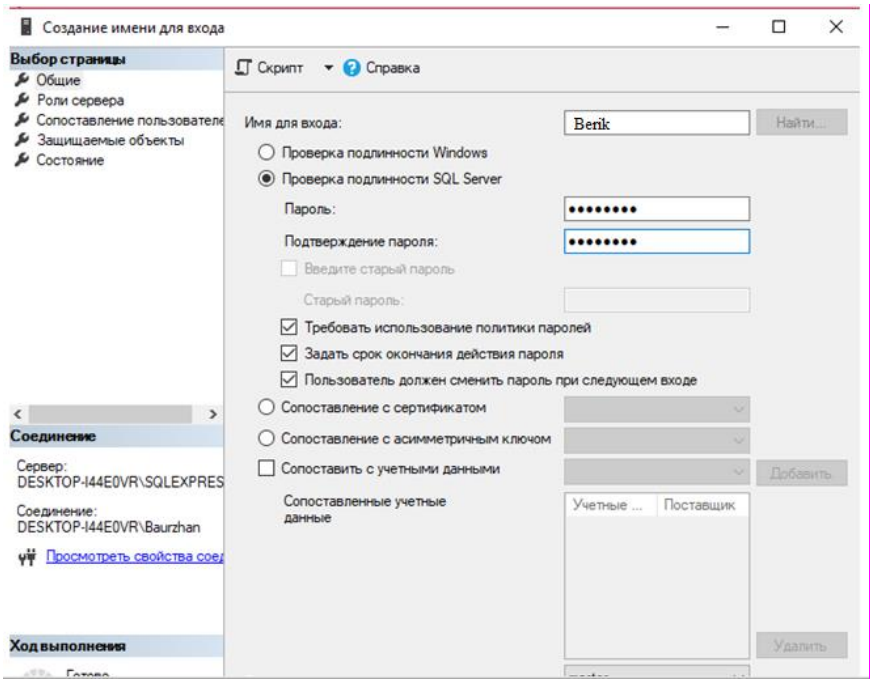


Сурет 62 – «Кіру аттарын құру»

1-тәсіл. Деректер қорын әкімшілендіру(63,64-сурет):



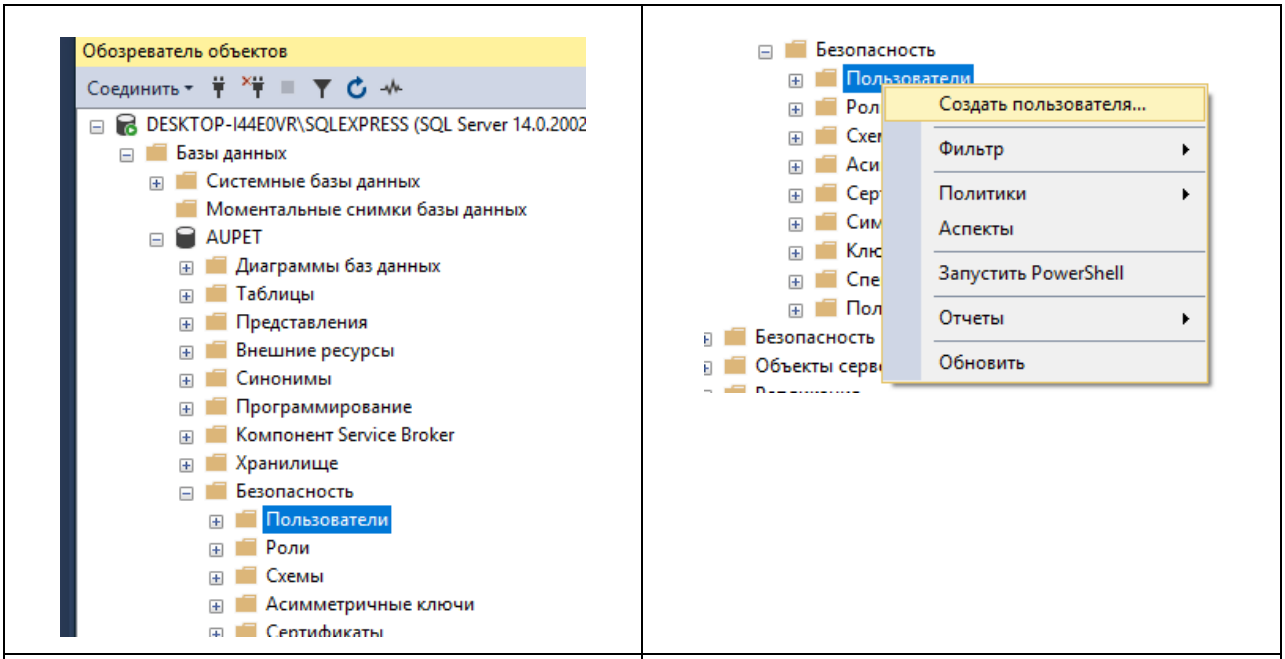
Сурет 63 – "Кіру аттарын" жасаған кезде көрсетілген интерфейс



Сурет 64 – кіру атын жасау мәзірі

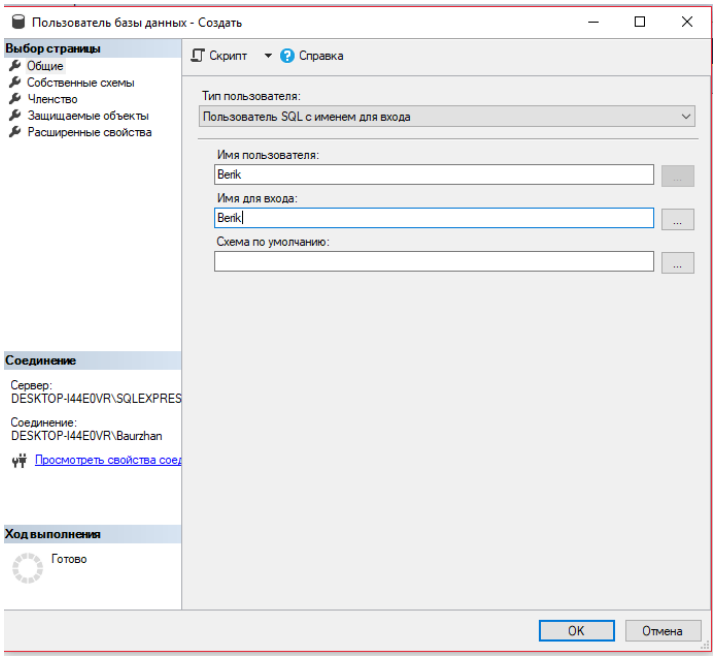
Шынайылығын тексеруді "SQL Server түпнұсқалығын тексеру" деп ауыстыру керек және кіру атын жасау қажет (65-сурет).

Кіру атын жасағаннан кейін оны нақты пайдаланушыға беру керек (65-суреттер).

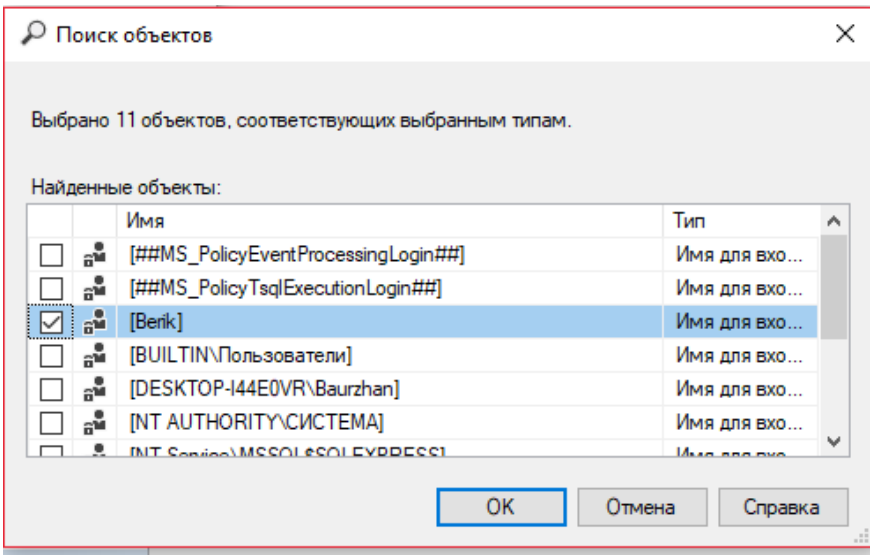


Сурет 65 (а,ә) – пайдаланушыны құру

"Пайдаланушының аты" өрісіне ДҚ-да танылатын атын жазып, Кіру атын беру керек (66,67-сурет)).

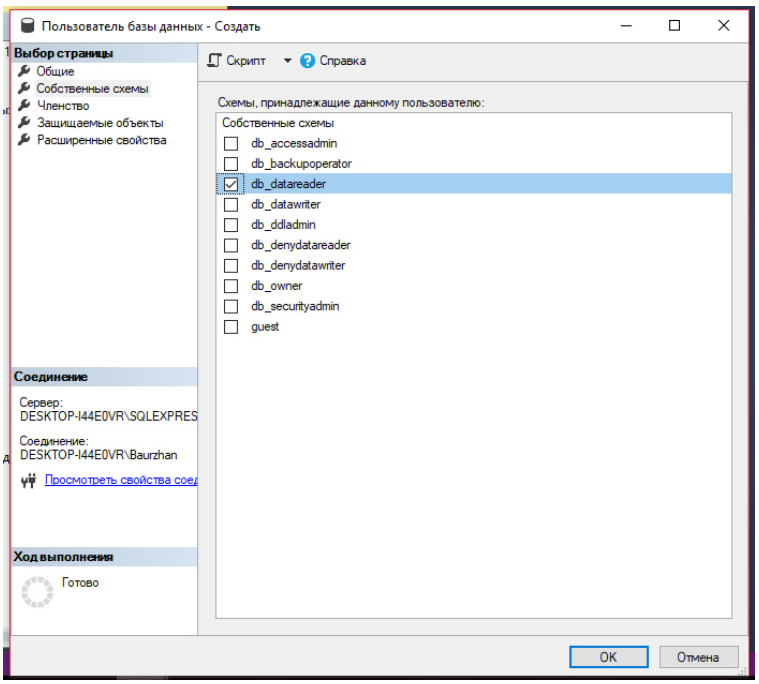


Сурет 66 – «Қолданушы атын құру»



Сурет 67 – " Кіру атын іздеу

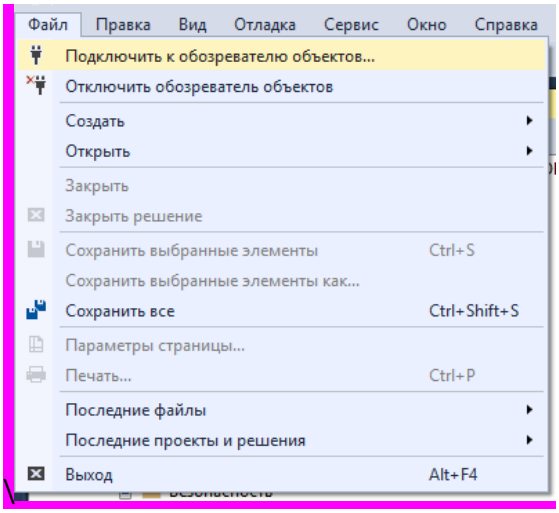
Деректер қорының сұлбасын және осы пайдаланушы үшін рөлді орнатамыз (68-сурет).



Сурет 68 – «Мүшелікті меншіктеу»

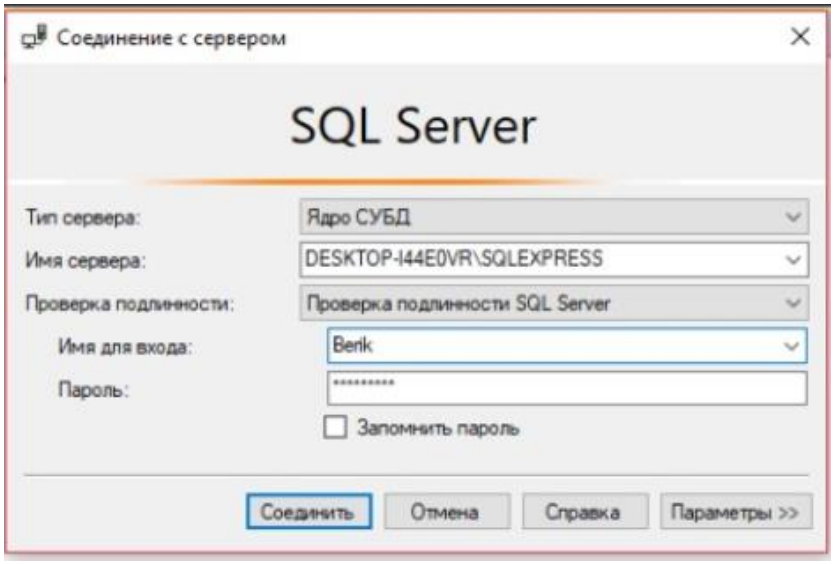
Әкімші атынан кіру:

Бұл әрекеттер пайдаланушыға ДҚ-да ұсынылған барлық деректерді оған қандай да бір өзгерістер енгізу құқығынсыз оқуға мүмкіндік беретін "db_datareader" рөлін беруге мүмкіндік берді. Тиісті пайдаланушының атымен ДҚ-ға қосылу үшін "Файл" менюінен "қойындыны" «Объектілерді шолғышқа қосу» салымын таңдау қажет " (69-сурет) [21].



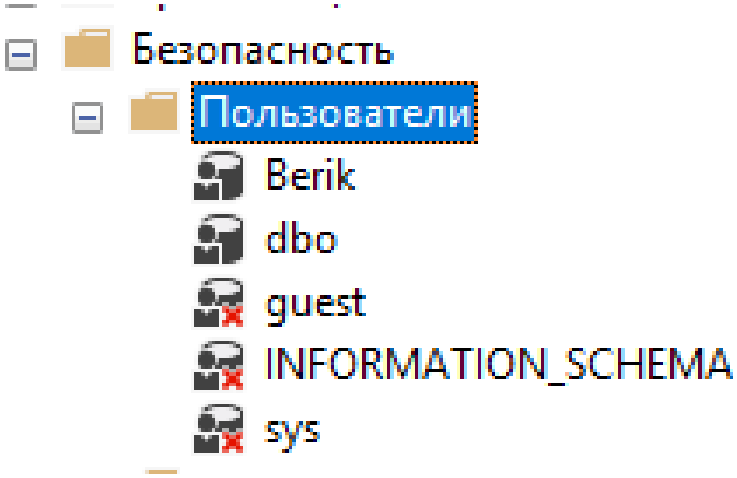
Сурет 69 – «ДҚ-ға қосылу»

«Түпнұсқалылықты тексеру» пунктінде (SQL Server түпнұсқалылығын тексеру» бөлімін таңдау (70-сурет).

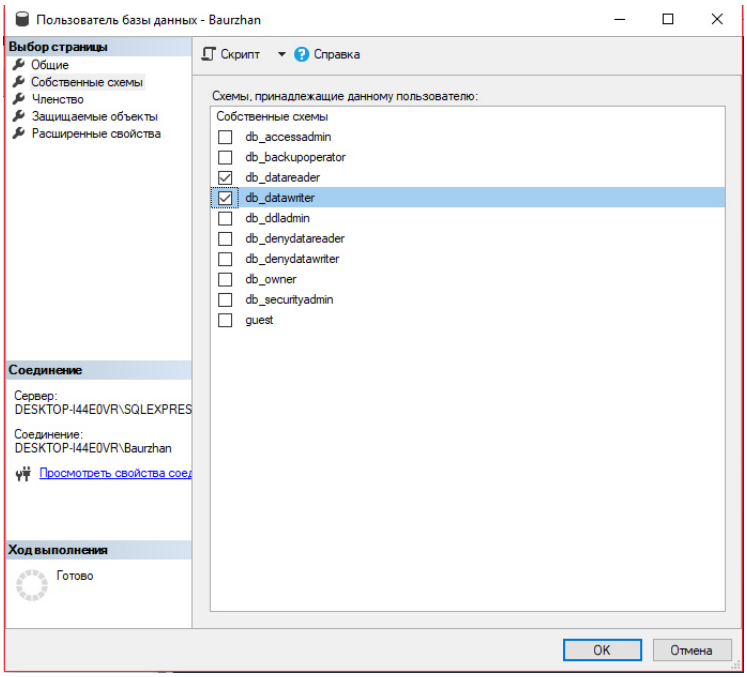


Сурет 70 – «ДҚ-ға қосылу»

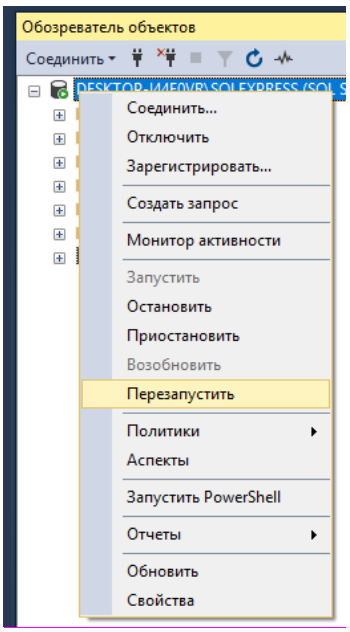
Баптау орындалғаннан кейін қайтадан Админ құрып тестілеу процесі орындалады(71-76-сурет)



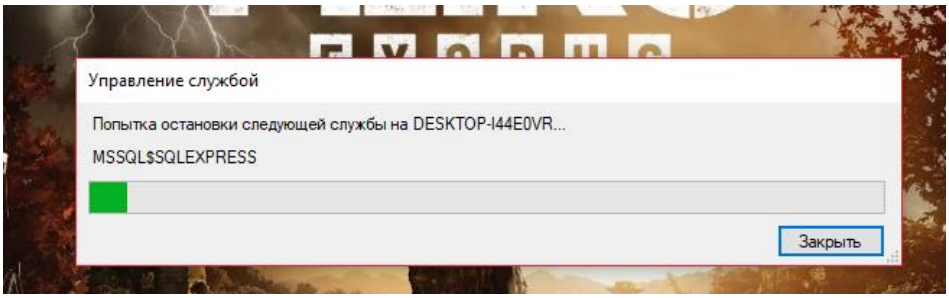
Сурет 71 – ДҚ-ға жаңа админ құрылды



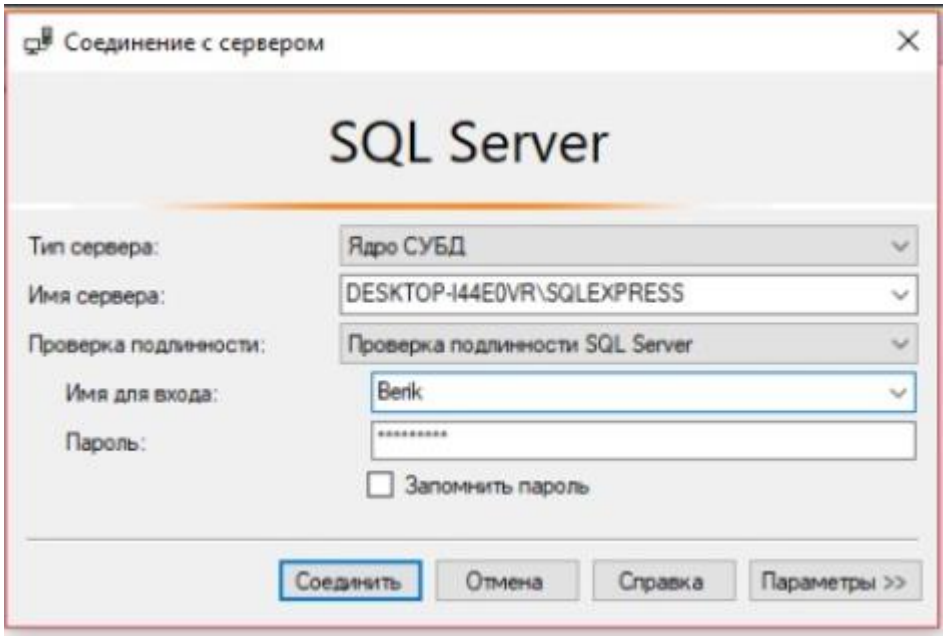
Сурет 72 – Қолданушылардың қолдану Атрибуттарын орнату



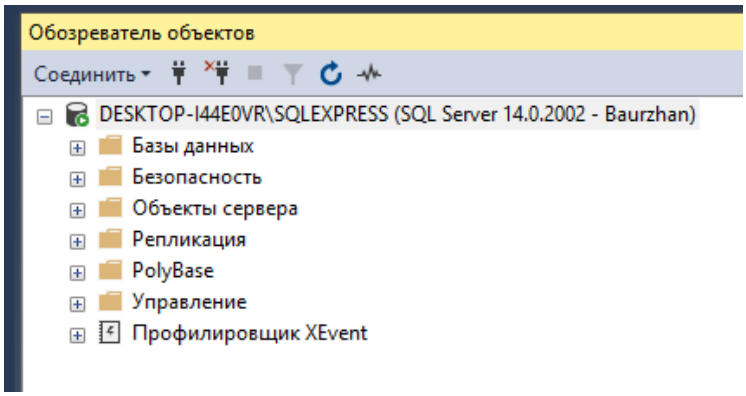
Сурет 73 – Қайта қосу процесі



Сурет 74 – админ құрылғаннан кейін прграмманы қайта жұмысқа қосу

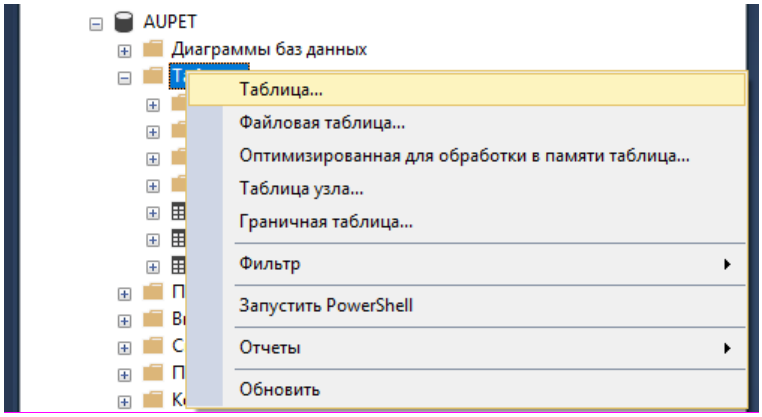


Сурет 75 – Әдминға кіру процесі

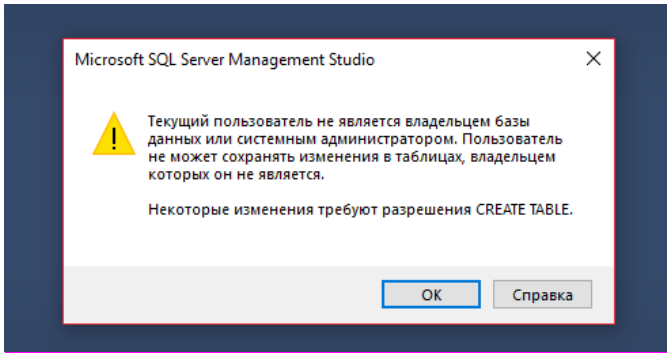


Сурет 76 – Кірген жағдайда, ДҚ ды редакциялап, оқи алатын мүмкіндік бар ма, соны тексеру процесі

3.2.1 Әкімшілендіруді тексеру(77,78-сурет)

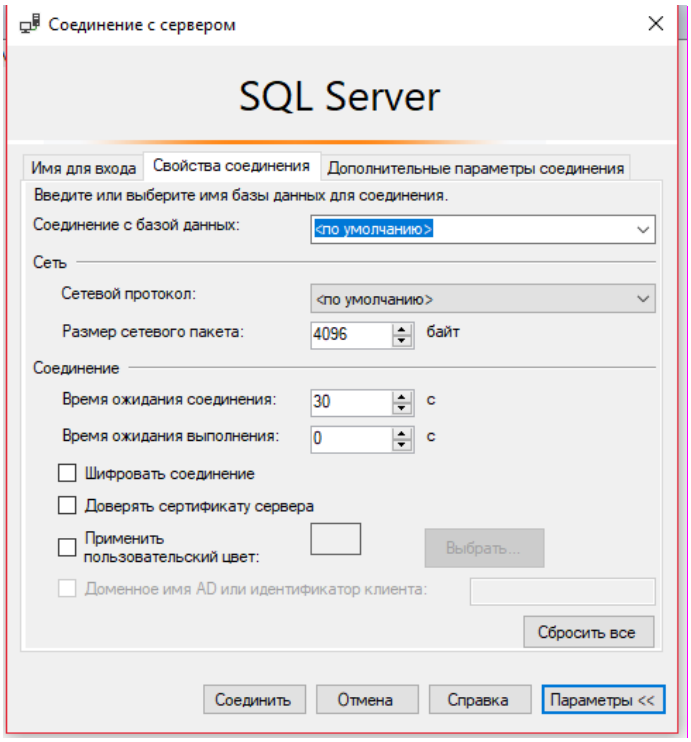


Сурет 77 – Нәтижесінде қолданушы деректер қорын аша аламайды, себебі оған админ құқығы берілмеген



Сурет 78 – Нәтижесі

2-тәсіл. Админді және Парольді қорғау(79-сурет):



Сурет 79 – Қосымша қорғаныс немесе қауіпсіздік орнату процесі

SQL-инъекциядан қорғау үшін сервермен қосылыс ұйымдастырылатын терезеде қосылыс параметрлерін дұрыс орнату керек, ол параметрлерге мыналар жатады:

- Қосылысты шифрлау;
- Сервер сертификатына сенімділік қалыптастыру;
- Қолданушы түсті қолдану.

Сервер сертификатына сенімділік қалыптастыру папаметрі мынадай мүмкіндіктерді жүзеге асыруға ықпал етеді, ол үшін мына процедуралар орындалу керек:

Выбрат батырмасын басып, PHP файлын таңдау. Осы файлдың ішінде қорғау механизмін жүзеге асыратын программалық код жазуға болады. Мысалы, программаны күрделі түрде қорғай аламыз, оған ақылы қорғау сатып алу мүмкіндігі жатады (Kazhackstan-ның күрделі қауіпсіздік шарасын қолдануға болады және т.б.) немесе өзіміз зашита құрай аламыз [21].

3.3 SQL-инъекциядан деректер қорын қорғау

SQL-инъекция (SQL-кодты енгізу) – еркін SQL-кодты сұрауға енгізуге негізделген деректер базасымен жұмыс істейтін сайттар мен бағдарламаларды бұзудың таралған тәсілдерінің бірі. SQL-инъекция қолданылатын ДБЖ түріне және енгізу шарттарына байланысты шабуылшыға деректер базасына ерікті сұрау (мысалы, кез келген кестелердің мазмұнын оқу, деректерді жою, өзгерту немесе қосу), жергілікті файлдарды оқу және/немесе жазу және шабуыл жасалатын серверде ерікті командаларды орындау мүмкіндігін алу мүмкіндігін бере алады. SQL-инъекциялар көп жағдайда осы ДБ-ға еркін SQL-

кодты енгізу арқылы ДБ-дан ақпаратты өзгерту, жою, қосу немесе оқу үшін пайдаланылады [23].

Әдетте, алдымен шабуылдаушы сервер скрипттерінің осалдығын іздеуді және сервердің аномалды реакциясына әкелуі мүмкін (мысалы, қате туралы хабарлама сияқты) түрлі сұраныстарды қалыптастыру арқылы ДБ құрылымын (кестелер, өрістер, жазбалар атаулары) қалпына келтіруді жүргізеді. Содан кейін ДБ құрылымы қалпына келтірілген кезде, онымен кез келген қажетті манипуляциялар жүргізіледі. Кез келген SQL-инъекциялардан ДБ әмбебап қорғау жоқ, бірақ сұрау салуларды бақылаудың кейбір стандартты әдістері бар: арнайы белгілерді экрандау, сұрау ұзындығын барынша кесу, параметрленген сұрау салуларды пайдалану, қолжетімділікті шектеу және т. б. төменде SQL-инъекцияның қарапайым мысалы берілген(80,81-сурет):

```
SELECT * FROM news WHERE id_news = 5
```

Сурет 80 – Сұраныс

```
SELECT * FROM news WHERE id_news = -1 OR 1=1
```

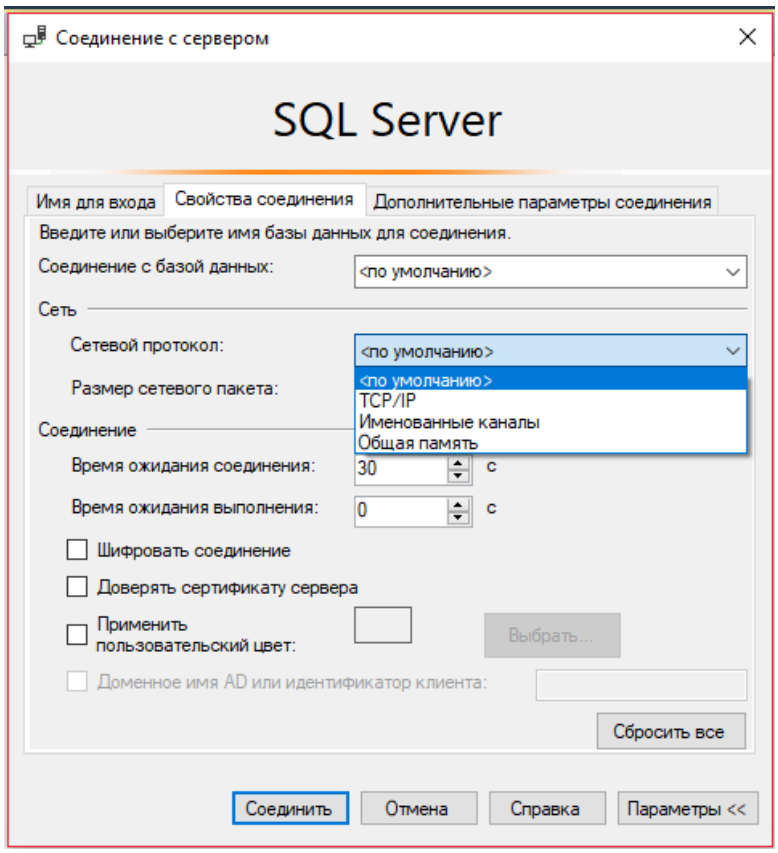
Сурет 81 – SQL-инъекция

1-суретте 5-ке тең id_news-тің параметрімен-news кестесін жазуды таңдайтын қарапайым сұрау үлгісі келтірілген. 2-суретте SQL-инъекция мысалы келтірілген, мұнда 5 мәннің орнына өрнек -- 1 OR 1=1. Бұл өрнек әрдайым шынайы (өйткені нақты өрнек -1=1) және сұрау нәтижесі осы кестенің барлық жазбаларын таңдау болып табылады. Осылайша, INSERT, DELETE құралы, DROP және т. б. командаларды қолдануға болады, бұл қорғалмаған сервердің ДҚ-мен кез келген қажетті әрекеттерді орындауына мүмкіндік береді.

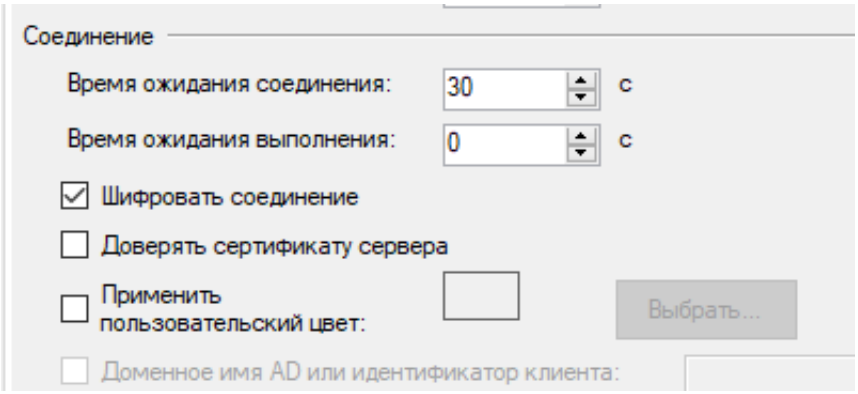
Осы сұранысты осындай SQL-инъекциядан қорғау үшін қажет(82,83-сурет):

1) Параметр id_news құралы тек бүтін мәндерді қабылдайды;

2) сұраныс ұзындығы шектелген (id_news параметрі үшін екі таңбалы сан).

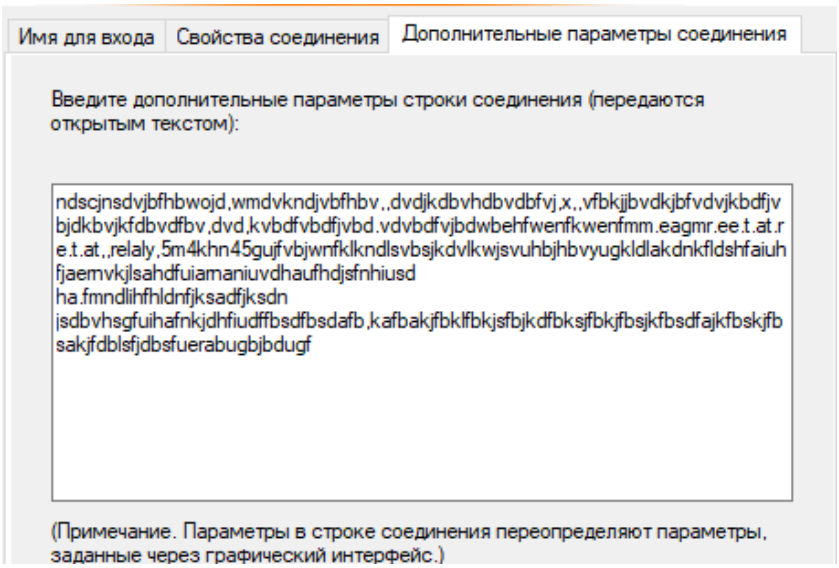


Сурет 82 – Желілік хаттама – IP таңдау



Сурет 83 – Қосылысты шифрлау

Қосымша қорғау – Электрондық цифрлық қолтаңба(84-сурет)



Сурет 84 – Қосылыстың қосымша параметрлер шифрланған түрде

SQL-инъекциядан қорғау

1) SQL инъекцияны болдырмау үшін екі қарапайым ережелерді сақтау керек. Деректерді өңдеусіз ДБ-ға орналастыруға болмайды. Мұны дайындалған өрнектер немесе қолмен өңдеу арқылы жасауға болады. Егер сұраныс қолмен қалдырылса, онда:

- барлық сандық параметрлер қажетті түрге келтірілуі тиіс;
- барлық басқа параметрлер mysql_real_escape_string() функциясымен өңделуі және тырнақшаға алынуы тиіс.

2) Пайдаланушы енгізген басқару құрылымдары мен идентификаторларды сұранысқа қойиау керек. Сценарийде алдын-ала ықтимал нұсқалардың тізімін жазып, тек оларды таңдау қажет [21].

MySQL сұраныстарын жасау ережелері

Егер біз сұрауға қандай да бір мәліметтерді қойсақ, бұл деректерді SQL командаларынан ажырату үшін оларды тырнақшаға алу керек. Мысалы, егер жазу болса база Bill – бұл басқа өрістің аты, оны таба алмайды және қате береді.

SELECT * FROM table WHERE name = Bill

Сондықтан, жалған мәліметтер (бұл жағдайда Bill аты) тырнақшаға жасалуы керек - онда дерекқор оны қатар деп түсінеді де өріске name-ді меншіктейді:

SELECT * FROM table WHERE name = 'Bill'

Дегенмен, деректердің өзінде де тырнақшалар да кездеседі. Мысалы,

SELECT * FROM table WHERE name = ' Д 'еканат'

Осы жерде дерекқор 'Д' – ны деректер, 'еканат'-ты түсініксіз команда деп ұғады да қате береді. Сондықтан барлық деректерді қадағалап отыру керек, сонда дерекқор тырнақшадағы деректерді *деректер* деп түсунетін болады. Нәтижесінде біз дұрыс сұраныс аламыз, ол қате тудырмайды:

SELECT * FROM table WHERE name = 'Д\'еканат'

Осылайша, біз сұрау салуға жол деректерін қою кезінде екі ережені ұстану керек екенін анықтадық:

- барлық енгізілетін жол мәліметтері тырнақшаға (бір немесе екі, бірақ ыңғайлы және жиі қолданылатыны дара тырнақша) алынуы тиіс.

- оларда арнайы символдар слешпен экрандалуы керек.

Ескерту: Слэштер ДҚ-ға қосылмайды. Олар тек сұраныстарда керек. ДҚ-да олар лақтырылып тасталады.

Жоғарыда айтылғандардың барлығы жол типтері мен мерзімдерге жатады. Сандарды тырнақшасыз қоюға болады. Егер сіз осылай істесеңіз, онда міндетті! сұрау салу алдында деректерді қажетті түрге келтіріңіз, мысалы:

$id=intval($id);

Бірақ қарапайым болу үшін (және сенімді) сандармен де жұмыс істеуге болады, жолдар сияқты (mysql оларды қажетті түрге түрлендіреді). Тиісінше, біз сұрау салынған кез келген деректерді қадағалап, тырнақшаға аламыз [21].

Сұраныстарды динамикалық құрастыру

Егер SQL сұраныс скрипте бүтіндей жазылса, және еш өзгермесе, онда ешқандай мәселе туындамайды

SELECT * FROM `table`

Бірақ біздің скриптердің барлық күші динамикалық сұраныстарды құрастыруда. Барлық жағдайға қажетті сұраныстарды жазудың орнына, біз скриптке түсетін деректердің негізінде оларды құраймыз. Міне, мұнда бізді қауіп-қатерден қорғайды. Мысалы, біз айнымалыны пайдалана отырып сұрау жасаймыз:

SELECT * FROM table WHERE name = '$name'

Ал егер $name бізде Д'еканат болса, сұраныс қате береді. Яғни, сұрау салу алдында өзгерісті желімдеу керек. Мұны бірнеше жолмен жасай аласыз. Ең қарапайымы (және дұрыс емес) – сиқырлы тырнақшаға салу. Сіз ойлағанындай, дәл осы жағдай үшін ойлап табылған. SQL сұраныстарын қатеден сақтау үшін скриптке түсетін барлық деректер талдаусыз желімделеді. Егер сіз бөтен кодты пайдалансаңыз, сиқырлы тырнақшаларды пайдалану жақсы. Бұл кейбір ыңғайсыздық тудыруы мүмкін және сізге қателесуден немесе бұзудан кепілдік бермейді (сұрауларды жасау ережесін сызумен аяқталмайды), бірақ ең болмағанда қауіп-қатерді төмендетеді. Сондықтан, бөтен кодты пайдаланғанда, сиқырлы тырнақшалардың қосылғанына көз жеткізіңіз. Егер сіз бүкіл кодты өз бетінше жазсаңыз, онда сұрауларды дұрыс жасауды үйрену керек [21].

Сұрау салу кезінде арнайы белгілермен дұрыс жұмыс істеу

Сұранысты дұрыс жасау үшін жоғарыда білгеніміздей, деректерді тырнақшаға жазып, оларды желімдеу керек. Біріншіден бәрі түсінікті. Динамикалық сұрауларды жасау кезінде біз барлық деректерді тырнақшаға жасауды ұмытпаймыз:

$query="INSERT INTO `table` VALUES(NULL,'$name','$date','$price')";

Егер $price айнымалы int типі болса және біз оны осы түрге келтіреміз, онда оны тырнақшаға алынбайды. Алайда, тырнақшаға алынса да, соншалықты қиындық әкелмейді. Тырнақша тек қатар ұзындығын анықтағанда қиындық туғызуы мүмкін. Бірақ деректерді шабуыл жасаушылардан қорғауда оладжы жаңылыстырудын жақсы тәсілі.

SQL Injection

Сонымен, біз деректерді дұрыс қоюды үйрендік. Бірақ, сұраныстарды динамикалық құрастыру деректерді қоюмен аяқталмайды. Бізге жиі SQL командасы мен өрістердің аттарына сұраныс жасауға тура келеді. Мұнда біз қауіпсіздік тақырыбына көшеміз:

SQL Injection – хакерлік шабуылдың бір тәсілі, онда скриптке берілетін деректер былайша модификацияланады: осмы скрипте қалыптасатын сұраныстар қызметі өзгереді. Шабуылдан қорғаудың екі түрі бар. Біріншісі-деректермен жұмыс, ол туралы жоғарыда айтылды, яғни тырнақша, слэштер қою арқылы деректерді өзгерту.

Екіншісі – сұраныстың басқарушы элементтерімен жұмыс. Бұл сәл күрделірек және біріншіге қарағанда әлдеқайда сенімді. Тырнақшалар арқылы кесте атын, SQL операторын, LIMIT командалары параметрлерін және басқак да операторларды қорғау мүмкін емес. Сондықтан негізгі ереже басқару элементтерін сұрау салу кезінде анықталады. Егер сұранысқа SQL операторлары немесе өріс, дерекқор, кесте аттарын динамикалық орнату қажет болса, оларды тікелей сұранысқа қандай түрде болмасын, салмау керек. Мұндай қосымшалардың барлық нұсқалары сіздің скриптыңызда алдын ала жазылып, пайдаланушы енгізген негізінде таңдалуы тиіс. Мысалы, егер өрістің атын order by операторына беру керек болса, онда оны тікелей қоюға болмайды. Алдымен оны тексеру керек. Мысалы, рұқсат етілген мәндер массивін жасау және осы массивте берілген параметр бар болса ғана сұраныс жасауға болады (хакерлік шабуыл дәл осы сұранысты аңдиды емес пе):

```
$orders=array("Date","Lesson","Teacher");
$key=array_search($_GET['sort'],$orders));
$orderby=$orders[$key];
$query="SELECT * FROM `table` ORDER BY $orderby";
```

Біз алдын ала сипатталған нұсқалардың массивінде пайдаланушы енгізген сөзді іздейміз, және, егер табылған жағдайда, массивтің тиісті элементін таңдаймыз. Егер сәйкестік табылмаса, массивтің бірінші элементі таңдалады. Осылайша, сұранысқа пайдаланушы енгізген нәрсе емес, бізде скриптте жазылған нәрсе қойылады [21].

4 Өмір тіршілігі қауіпсіздігі

4.1 Компьютердің жұмыс кезіндегі қауіпсіздігі

Компьютер – адам интеллектінің ең тамаша жетістіктерінің бірі. ЭЕМ және ДК үлкен ресурстары арқылы қолданушылардың тікелей диалог жүргізе алу мүмкіндігі миллиондаған адамдардың экран алдында көп уақыт өткізуіне алып келді. Уақыт өте келе компьютер пайдаланушыларында өздерін сезінуге байланысты шағымдар жиынтығы пайда болады.

Бұл компьютерден адамның денсаулығына сәулеленудің әсері туралы ойлаға алып келді. Мұндай ойлар үшін көптеген себептер бар. Бірқатар ғалымдар тұрмыстық АЖЖ көздерінен адамдарға электромагниттік сәулеленудің әсерімен байланыстырады.

Электрондық құрылғылар әртүрлі түрдегі сәуле шығарады – электромагниттік толқындар, электростатикалық кернеу және радиация. Электростатикалық кернеу электрді пайдаланатын барлық құрылғыларда болады, оның негізгі көздері – электр беру желілерін құрады. Қалада тұрып, одан құтылу мүмкін емес, компьютерлерден сәулелену осы әсерден аз көлемді құрайды. Сондықтан электромагниттік толқындарға толығырақ тоқтай кетсек.

Олар сезілмейді, денсаулыққа айтарлықтай зиян әкелмейді, бірақ дүниежүзілік денсаулық сақтау ұйымы экология үшін қауіпті факторлардың тізіміне электромагниттік сәулені енгізді. Электр желісінен жұмыс істеу кезінде аспаптар Жерді қоршаған физикалық өрісте импульстердің тербелісін жасайды. Бұл тербелістер экожүйенің жай-күйіне теріс әсер ете отырып, ғаламшардың жалпы электромагниттік өрісінің қозуын тудырады. Ал үйде компьютерден зиянды сәулелену денсаулыққа теріс әсер етуі мүмкін.

Әрбір дербес компьютерден электромагниттік сәуле шығады: төмен жиілікті және радиожиілікті. Дүниежүзілік денсаулық сақтау ұйымының пікірінше, толқындардың екі түрі де канцерогенді болып табылады – ол обыр ауруын тудыруы мүмкін. [22]

4.1.1 Компьютер мониторынан бөлінетін сәулелер

Мониторлардың ішінде электронды – сәулелі түтікшелілері ең зиянды екені анықталды. Олады пайдаланған кезде, компьютер сәуле шағарады ма деген сұрақ туды. Иә, монитордан бөлінетін радиацияның зиянын рентген сәулелерінің зиянымен салыстыруға болады. Құрал 2 және одан да көп сағат компьютерді өшіргеннен кейін де сақталатын қуат өрістерін және жоғары электр кернеуін шығарады.

Сұйық–кристалды мониторлар айтарлықтай қауіпсіз, олар шамамен 50 Гц сәулелендуді қалыптастырады. Бұл доза ағзаға нақты зиян келтіру үшін аз, бірақ тұрақты әсер ету кезінде жағымсыз салдарлардан қашып құтылу мүмкін емес. Аналық плата мен корпустың қызуына байланысты ауаның деионизациясы және қоршаған ортаға зиянды заттардың бөлінуі орын алады. Міне, сондықтан тұрақты жұмыс істейтін есептеу техникасы бар бөлмелердегі ауа тыныс алу үшін өте ауыр. Тыныс алу жүйесі әлсіз адамдар үшін бұл

фактор демікпені тудырып, кері әсер етуі мүмкін. Ол компьютердің электростатикалық өрісінің және монитордың ауадағы өлшенген шаң бөлшектеріне әсерімен одан әрі күрделене түседі. Электрленіп алып, олар "тозаңды коктейль" құрайды, тыныс алуды ауырлатады.

Сенсорлы экранның болуы радиацияның жоқтығына кепілдік бермейді. Себебі, сіздің саусақтарыңыз экранда манипуляциялар жасай отырып, онымен, wi-fi-антеннадан бірнеше миллиметрде жанасады.

Әсіресе, жол жағдайында жұмыс істеуге арналған портативті құрылғы ретінде ойланған ноутбук сәуле шығару мәселесін де назарсыз қалдыруға болмайды. Бұл ыңғайлы және көпфункционалды құралдарды толық жұмыс күні ішінде пайдалану әртүрлі патологиялар мен аурулардың себебі болуы мүмкін. Өйткені, ол қарапайым компьютер сияқты электромагниттік сәулелену көзі болып табылады, бірақ ол адамға компьютерден айтарлықтай жақын орналасады. Сол себепті, олардың ада ағзасына зияны да көбірек.[3]

Жүйелік блок өзі айналасында электромагниттік өрісті белсенді жасайды. 2 мгтс (миллигаусс) минималды фондау ағзаға теріс әсер етеді. Ол адамнан 50-ден 100 см-ге дейінгі қашықтықта орналасқан құрылғы тудыра алады. Процессор неғұрлым жақынырақ болса, соғұрлым күшті әсер етеді.

Олар ерекше қауіп тудырады, өйткені әрқашан басқа тікелей киіледі. Сымсыз гарнитуралар мен Bluetooth жүйелері – бұл ең нашар нұсқа: олар арқылы адам ағзасына радио толқындары да енеді. Кабель айтарлықтай қауіпсіз, бірақ ұмытпаған дұрыс: оның ішінде металл – компьютер процессорынан тікелей кез келген сәулелер үшін тамаша өткізгіш. Жалпы, құлаққаптарды алып тастау және колонкадан дыбыс шығару мүмкіндігі пайда болған соң, оны бірден пайдаланған жөн.

Кейбір қуатты колонкалар, әсіресе вуферлер айналасында елеулі электромагниттік өріс жасайды. Олардан кемінде 50 см қашықтықта ұстаған жөн.

Мөлшері әртүрлі және тиісінше қуаты бар. Ең қарапайым, үй принтері 50 см қашықтықта ұстаған дұрыс. Үлкен кеңсе үшін арналған принтерді адамдардан 65 см арақашықтықта қалдыру керек.

Олардың радиожиілік магнит өрістері айнала көп метрге созылады. Бұлар сонысымен ыңғайлы, бірақ денсаулық үшін зиян. Тіпті егер оларды компьютерге кабель арқылы қосқан күнде де – төмен жиіліктер адамға әсер етеді. Сондықтан оларды 35 см кем емес қашықтықта қою керек.

Олар жоғарыда аталған барлық техника үшін өте қуатты төмен жиіліктерді шығарады. Оларды бір метр қашықтықта ұстау керек.

4.2 Компьютерден бөлінген сәулелердің адамға әсері

Компьютерден бөлінетін сәулелердің адам ағзасына неге зиянды екенін анықтайық.

Адам ағзасы да электрлік импульстерді шығарады. Олардың көмегімен ми мен жұлынға жүйке үштары арқылы сигналдар келіп түседі, қаңқа бұлшықеті мен жүрек бұлшықеттері азаяды. Жүйке үштары арқылы

секундына мыңдаған сигналдар беріледі, сондықтан компьютерден қандай зиян келетінін оңай түсінуге болады, сәулелер электрлік импульс жіберудің қиын жүйесіне әсер етіп, олардың өзара байланысына бөгет келтіруі мүмкін. Оның әсері бір сәтте сезілмейді,ол ағзада жинақталып, мүшелер мен жүйелердің жұмысын біртіндеп нашарлатады.

Екі маңызды жүйе ең осал болып табылады:

- жүйке жүйесі
- жүрек – қан тамырлар жүйесі.

Бұның әсерінен ми сигналдары патологиялық түрде өзгеруі мүмкін. Бұл мидың және жүрек-тамыр жүйесі органдарының бұзылуына себеп болады. Жүрек-қантамыр жүйесінің қалыпты жұмыс істеуі импульстердің когеренттігіне және беріктігіне байланысты. Үйдегі бір немесе одан да көп құрылғылар жүрек жұмысын елеулі бұзылуға алып келмейді, бірақ үнемі сәулелену аритмия мен жүрек-тамыр қабілетінің бұзылуына әкелуі мүмкін. Ұзақ уақыт бойы әсер етуі бас ауруы, мигреньдер, иммунитеттің төмендеуі, депрессия, гормоналды теңгерімсіздік және ұйқының бұзылуына әкелуі мүмкін. Компьютерде көп жұмыс істеу Альцгеймер ауруы, Паркинсон ауруы, қатерлі ісік ауруы және ұрпақты болу жүйесінің бұзылу қаупін арттырады. Сонымен қатар миокард және перикард ауруларына, ағзаның жалпы гормональды фонының бұзылуына, су-тұз алмасуының нашарлауына, гомеостаздың бұзылуына алып келуі мүмкін.

Үй компьютері, ноутбук немесе смартфон зиянды сәуле көзі болып табылады. Компьютерден қанша сәуле алатынымыз түрлі факторларға байланысты: құралдың түрі, пайдалану уақыты, орналасуы. [23]

4.3 Сәулеленуден қорғанудың іс-шаралары

Компьютерден қандай сәуле бөлінетінін және оның адам ағзасына калай әсер ететінін анықтаған соң, одан қорғану шараларын қарастыра кетсек.

Келесі кеңестерді орындай отырып, компьютерден бөлінетін сәулелердің әсерін бәсеңдетуге болады:

- егер бірнеше компьютер немесе ноутбуктер үнемі бір үй-жайда (мысалы, сыныпта, кеңседе) тұрса, оларды құрылғылар бөлменің периметрі бойынша тұратындай, ал орталық бос болатындай етіп орналастыру керек;
- мүмкіндігінше электрмагниттік сәулеленудің саны мен қарқындылығын азайтатын арнайы қорғаныс құралдары орнатылған мониторларды пайдаланған жөн. Әсіресе, бұл кеңес компьютер алдында көп уақыт жұмсайтын балаларға өзекті болып табылады;
- мониторды таңдау барысында, оның кеңеюіне, қорғау деңгейіне және радиациялық сәулелену мөлшеріне назар аудару керек. Low Radiain жазуы бар экрандарға көбірек назар адару қажет, себебі бұл ең аз радиация санын білдіреді;
- монитор көру үшін ыңғайлы қашықтықта, ал жүйелік блок пайдаланушыдан барынша алыста орналасуы тиіс;

- жұмыс аяқталғаннан кейін компьютерді өшіру керек, өйткені ол қаншалықты ұзақ жұмыс істесе, соғұрлым көп сәуле шығарады және ауаны арқылы қоршаған ортаға зиянды заттардың үлкен мөлшерін бөледі;

- арнайы қорғаныс пленкасын пайдалану электромагниттік сәуле шығару қарқындылығын және пайдаланушы ағзасына зиянды әсер ету мөлшерін азайтады;

- шаңды жүйелі түрде шығару, ылғалды жинау және мүмкіндігінше ионизаторларды қолдану компьютер жұмысының нәтижесінде алынған заттар әсер ететін дем шығаратын ауаның сапасын жақсартады, сондай-ақ адамның денесіне электромагниттік сәулеленудің зиянды факторларының әсерін азайтады;

- монитордың жандарынан және артқы бөлігінен шығатын сәулелер компьютермен бір бөлмеде, бірақ оны қолданбайтын адамға әсер етпеуі үшін, оны бөлменің бұрышына орналастырған жөн. Сондай-ақ, монитор көзге ыңғайлы жағдайда (бірақ кемінде 40 см) болуы тиіс, ал жүйелік блок пайдаланушыдан мүмкіндігінше алыс орналасуы тиіс.[24]

4.4 Қолданушының компьютерден қауіпсіздік қашықтығын есептеу

Компьютер алдында жұмыс жасау барысында, барынша қауіпсіздікте болу үшін, монитордан көзге дейінгі ең аз арақашықтықты білу керек. Егер монитордың экраны қолданушыға қатысты дұрыс орналасса, қолданушының жақсы көру қабілетін ұзақ сақтап, остеохондроз және омыртқаның қисаюын болдырмайды.

Монитор мен көздің арасындағы қашықтық, ең алдымен, оның өлшемді параметрлеріне байланысты. Қазіргі уақытта ең танымал модельдер 14 – тен (ноутбуктар) 27 дюймге дейінгі диагоналдармен, ал ең үлкені диагоналі 30 – дан асатын экрандармен жабдықталған. Мониторлардың техникалық мүмкіндіктері мен қолдану салалары олардың дюйм өлшемдеріне байланысты.

Ең көп таралған модельдер келесі түрде болады:

1) 14-16''. Бұл бұқаралық ноутбуктар, олардың өлшемдері оңтайлы өнімділікті процессорларды ендіруге мүмкіндік береді. Кішкентай диагоналды портативті құрылғылардың қолданыс аясы тар.

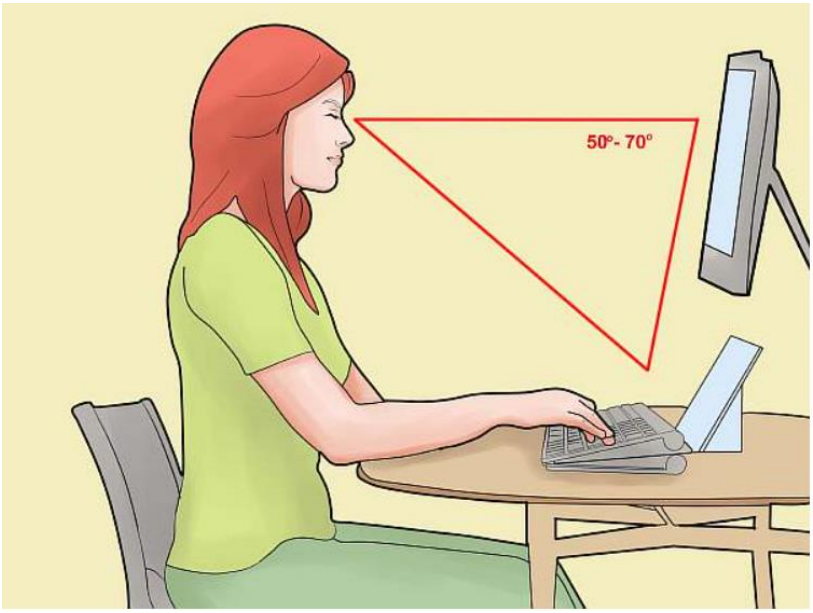
2) 17''. Көлемді ноутбуктар кеңсе үшін ыңғайлы нұсқа. Алып жүру ыңғайлы болмағанымен, жұмыс аймағында кеңістікті үнемдйді.

3) 18,5-20,1''. Шағын стационарлы модельдер, көбінде мәтін редакторында жұмыс жасау үшін пайдаданылады.

4) 21,5-24''. Орташа диагоналды бейнемониторлар қолданушыға ыңғайлы түрде мәтін теруге, бейнебаяндарды редакциялауға, бейнефильмдерді көруге мүмкіндік беретін әмбебап нұсқа болып табылады. 3D бейнесі бар ойынды қолдау үшін диагоналі кемінде 23 дюйм болуы керек.

5) 27'' және одан жоғары. Олар көбінесе фильмдер көруге, фото, бейне, аудио материалдырды редакциялау үшін қолданылады. Бұл мониторлар студияда, әсіресе, дыбыс жазу және фильм түсіру барысында таптырмас құрал

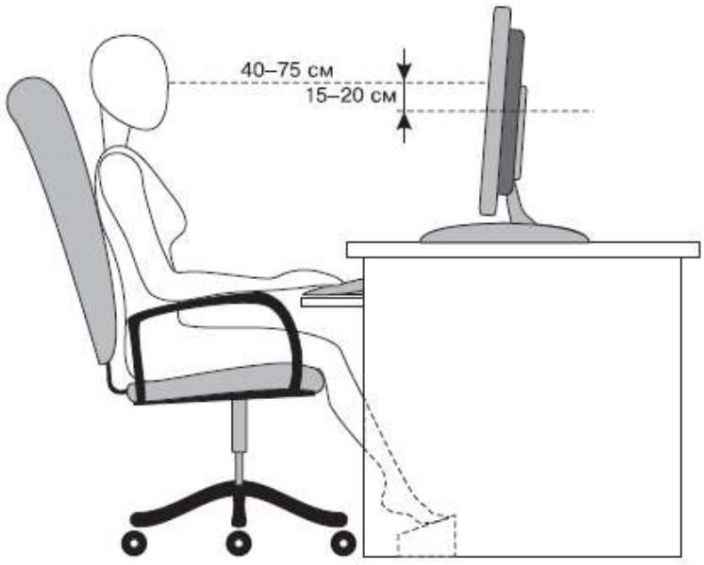
болып табылады. 32 және одан да жоғары дюймді мониторлар бейнебақылау үшін пайдаланылады. Ал қабырға мониторын теледидар ретінде пайдалану керек болса, оның диагоналі 31 – 34 дюйм болғаны жөн(85-сурет).



Сурет 85 – Компьютер үстелінде

Ғылыми зерттеулерге сүйенсек, адамның көзі 17 градус шеңберіндегі кескінді анық көре алады. Бұл жауап математикалық т.рде алынады: пайдаланушының беті мен экран арасындағы ең аз рұқсат етілген қашықтық оның диагональды ұзындығы болып табылады.

Көз бен бейне монитор арасының қанша сантиметр болу керек екенін анықтағанда, оның өлшемдерін ғана емес, сонымен қатар жобалау ерекшеліктерін де ескеру қажет. TFT панелі бар СК-дисплейді қолдану қауіпсіздірек(86-сурет) [25].



Сурет 86 – Нормативті арақашықтық

Электронды-сәулелік түтікке негізделген дәстүрлі құрылғылармен салыстырғанда, СКД үлгілері мынадай артықшылыққа ие:

- элетромагниттік сәулеленудің өте аз мөлшерде болуы;
- көрінетін аймақтың үлкен өлшемі (15 дюймдік СКД мониторы 17 дюймдік CRT аналогы сияқты);
- сурет бұрмалауының жоқтығы;
- үстелде үнемді орын алуы.

CRT бар болған жағдайда компьютер мониторынан 60-70 см қашықтықта болу керек, ал СКД барлық шарттарға қарамастан арақашықтықты 30-50 см қысқартуға мүмкіндік береді. Көзге түсетін жүктемені азайту үшін кескінді дұрыс бейідеу маңызды, сонымен қатар, бірінші мониторды арнайы бағдарлама арқылы тексеріп алған жөн.

Медициналық стандарттарға сәйкес, компьютерлік мониторға оңдайлы қашықтық ең аз дегенде бір жарымнан екі диагоналға дейін болуы керек. Есептеу үшін келесі формула қолданылады:

$$S – L * 2,54 * 1,75 \quad (4.1)$$

мұнда,

L –диагональдың дюймдік ұзындығы;

2,54 – дюймді сантиметрге айналдыру коэффициенті;

1,75 – 1,5 және 2 диагоналі арасындары арифетикалық орта.

Формулаға сәйкес диагоналі 17 дюйм болатын кеңсе ноутбугынан оңтайлы қашықтықты есептесек:

$$S = 17 * 2,54 * 1,75 = 75 \text{ см} \quad (4.2)$$

Компьютерлердің әртүрлі модельдері бойынша есептеулердің нәтижелері 4.1-кестеде келтірілген.

Кесте 4.1 – Компьютердің модельдеріне қатысты есептеулер

Диагоналдың өлшемі, дюйм	Экраннан көзге дейінгі оңтайлы қашықтық, см
14	62
15	67
16	71
17	75
18	80
19	85
20	89
21	94
22	98
23	102
24	107
25	111

4.1-кестенің жалғасы

26	116
27	120
28	125
29	129
30	134
31	138
32	142
33	147

Студенттер мен оқушылардың, операторлардың, қызметкерлердің еңбекгін қорғау мақсатында олардың монитор алдындағы жұмыс орнын SanPiN 2.2.2.542 – 96 және SanPiN 2.4.2.1178 – 02 санитарлық нормалары және ережелеріне сай жабдықталуы керек. Бұл мәселеге құзіретті көзқарас визуалды шаршау мен басқа да аурулардың алдын алуға көмектеседі.

4.4.1 Бақылау жүйесі үшін мониторларды орналастыру

Қазіргі кезде кәсіпорындардың, мекемелердің немесе дүкендердің қорғалуы мен басқаруы бейнебақылау арқылы жүзеге асырылуда.

Тағы бір маңызды ерекшелігі – бір дисплейдің бірнеше камераларда жұмысы болып табылады, яғни, камералардың әрқайсысы белгілі бір аймақта орналасқан және әрбіреуі өз бейнесін көрсетеді (бейне өрісі). Дисплейді тиімді бақылау үшін 20-24 өріс болғаны жөн деп саналады.

Қажетті санына қарай бейнеқұрылғының диагоналын есептейді, шыққан мәнге сүйене отырып экранның бақылаушы көзіне дейінгі арақашықтықты есептейді. Барлық үш параметрдің дұрыс коэффициенттері 4.2-кестеде келтірлген.

Кесте 4.2 – үш параметрдің дұрыс коэффиценттері

Өріс саны	Диагональ ұзындығы, дюйм (см)	Бақылаушы мен дисплей арасындағы қашықтық, м
4	Минималды – 17 (43)	1,7
9	19-дан 22-ге дейін (50 – 56)	2,0
16	19-дан 40-қа дейін (50-102)	2,0-3,0
20	Ең аз 32(81)	2,5

4.4.2 Компьютер аудиториясында мониторларды орналастыру ережесі

Аудиторияны жоспарлау кезінде копмьютерлік аудиторияның ішіндегі жұмыс орындарын шектеуді ұсынатын санитарлық норманың SanPiN 2.2.2.542-96 SanPiN 2.4.2.1178-02 пунктілері ескерілуі тиіс. Бір қолданушыға

арналған алаң 2,5-тен 3,5 $м^2$-ге дейін болуы керек. Бір компьютер үшін рұқсат етілген ең аз аймақ 6 $м^2$ жетеді.

Аудиторядағы жұмыс орындары үш жолмен ұйымдастырылады:

- қатар түрінде қолданушылар бір-бірінің артында отырады, барлық дисплейлер бір бағытта бұрылады;
- кеңсенің ортасында компьютері бар үстелдердің екі қатары аудиторияның ортасыда бос орынсыз орналасады, ал компьютерлердің экрандары бір-біріне теріс бағытта айналдырылады;
- периметр бойынша – компьютері бар үстелдер қабырға бойымен орналастырылады.

Жұмыс орнын жабдықтау кезінде пайдаланушы көзінен монитор экраны кемінде 50-70 см қашықтықта болуы керек. Пайдаланушының үстелде дұрыс отырғаны жөн. Сонымен қатар, келесі ескертулердің де назарсыз қалмағаны дұрыс:

- дисплей жазықтығы тігінен орналасса, оның орталығы (немесе 2/3 биіктігіндегі нүктесі) көздің деңгейінде орналасу керек;
- көздің экранға 90 ˚ бұрышпен түскені жөн(перпендикулярдан 5-10˚ ауытқу рұқсат етіледі);
- бас аздап алға қарай қарағаны дұрыс максималды 15˚ [26].

Бұл шарттар үшін 4.3-кестені қолданған дұрыс.

Кесте 4.3 – Жұмыс орнын жабдықтау

Қолданушының бойы, см	Үстел бетінің еденнен қашықтығы,см	Орындықтың еденнен қашықтығы, см	Орындық тереңдігі, см
100 – 115	46	26	26
115 – 130	52	30	29
130 – 145	58	34	33
145 – 160	64	38	36
160 – 175	70	42	38
175 – тен көп	76	46	40

Жоғарыдағы ережелерге сүйене отырып, қолданушы өзіне сәйкестендіріп монитордың орналасу орнын жабдықтай алады. Келтірілген ережелерді сақтау омыртқаның тіктігіне және көз саулығына көп септігін тигізеді.

5 Техникалық-экономикалық негіздеме

5.1 Жобаның сипаттамасы

Менің дипломдық жобамның мақсаты бағдарламалық қамтамасыз етуді әзірлеу.

SQL инъекция сияқты маңызды осалдықтардан қорғау үшін.

Осы бағдарламалық қамтамасыз етуді әзірлеу кезінде (брандмауэр) келесі мамандар жұмыс жасайды: жоба менеджері және бағдарламашы-әзірлеуші. Жобаның менеджерінің міндеттері жұмыс кестесін тексеру және олардың сәйкестігін қамтиды. Бағдарламашы-әзірлеуші, өз кезегінде, техникалық негіздемені, бағдарламалық қамтамасыз етуді, тестілеуді және техникалық қызмет көрсетуді әзірлеуі керек.

Менің жұмысымның дамуы мен енгізілуінің техникалық-экономикалық негіздемесі мыналарды қамтиды:

- даму бағдарламасының күрделілігін анықтау;
- бағдарламаның дамуын есептеу;
- әзірленген бағдарламаның ықтимал бағасын анықтау;

5.2 БӨ әзірлеудің еңбек сыйымдылығы

Бағдарламалық қамтамасыз етуді әзірлеудің күрделілігін дәл анықтау үшін тапсырмаларды кезеңдерге бөлу керек. Бағдарламалық қамтамасыз етуді әзірлеудің және дамудың күрделілігінің үлестіру үлгісі 5.1-кестеде келтірілген.

Кесте 5.1 – БӨ әзірлеу кезеңдері

БӨ әзірлеу кезеңдері	Жұмыс түрі	БӨ әзірлеудің еңбек сыйымдылығы, адам саны х сағ.
1 кезең	Тапсырманы қою	12
2 кезең	Тақырыпты шолу	12
3 кезең	Деректер базасына қатерлерді талдаудың қолданыстағы әдістерін іздеу және зерттеу	14
4 кезең	Дерекқорларға қауіп-қатерді болдырмау, болдырмау және жою жолдарын іздеу	5
5 кезең	Бағдарламалық қамтамасыз етудің теориялық бөлігін құрастыру	18
6 кезең	Деректер базасында ақпараттық қауіпсіздікті енгізу	24

5.1 кестенің жалғасы

7 кезең	Даму ортасын таңдау	6
8 кезең	Бағдарламалау тілін таңдау	5
9 кезең	Бағдарламалық қамтамасыз етуді жазу	35
10 кезең	Жобаны қайта белсендіру	30
11 кезең	Жобаны іске асыру	25
12 кезең	Атқарылған жұмыс туралы есеп жасау	10
13 кезең	Өнімді тестілеу	12
Қорытынды	жобалық жұмысты орындаудың еңбек сыйымдылығы	218

Жұмыс күнінің ұзақтығы 8 сағатқа тең. Нәтижесінде бағдарламалық қамтамасыз етуді іске асыру үшін 28 жұмыс күні қажет.(218/8≈28)

5.3 БӨ әзірлеуге арналған шығындарды есептеу

Бағдарламалық өнімді әзірлеу үшін қажетті шығындарды анықтау қолда бар ақпарат негізінде жүргізіледі, ол мынадай элементтерді қамтиды:

- материалдық шығындар;
- еңбекақы төлеу шығындары;
- әлеуметтік салық;
- негізгі қорлардың амортизациясы.

Материалдық шығындар негізгі және қосалқы шығындарға, энергияға және БӨ әзірлеуге қажетті басқа да шығындарға бөлінеді. Материалдық шығындарды есептеу 5.2-кестеде берілген нысан бойынша жүргізіледі.

5.2 кесте – материалдық ресурстарға шығындар

Материалдың атауы	Өлшем бірлігі	Саны	Бірлік үшін баға, теңгемен	Соммасы, теңгемен
Кеңсе қағазы	Қаптама	1	1 300	1 300
Дәптер (48 бет)	Дана	2	120	240
Қалам	Дана	2	100	200
Компьютер тінтуірі	Дана	1	4 000	4 000
Қорытынды				5740

Материалдық құралдарға ($З_м$) қажетті жалпы соманы мынадай формула бойынша есептеуге болады:

$$З_м = \sum P_i * Ц_i, \quad (5.1)$$

мұнда P_i – материалдық ресурстың і түрінің шығысы, заттай бірліктер;

$Ц_i$ – материалдық ресурстың і түрінің бірлігінің бағасы, тг;

I – материалдық Ресурстың түрі;

N – материалдық ресурстар түрлерінің саны.

Бағдарламалық қамтамасыз етуді әзірлеу үшін Lenovo Z710 ноутбугі пайдаланылатын болады.

Қажетті жабдықтар мен бағдарламалық қамтамасыз ету шығындарын есептеу 5.3-кестеде келтірілген нысан бойынша жүргізіледі.

5.3 кесте – жоба үшін қажетті жабдыққа арналған шығындарды есептеу

Материал атауы	Өлшем бірлігі	Саны	Бірлік үшін баға, тг	Қорытынды, тг
Принтер	Шт	1	35 000	35 000
Ноутбук Lenovo G50	Шт	1	343 000	343 000
Модем	Шт	1	10 000	10 000
Қорытынды				388 000

Зм = 388 000 + 5740 = 393 740

Бағдарламалық өнімді әзірлеу үшін 393 740 теңге сомаға материалдар қажет.

5.4 Электр энергиясына арналған шығындарды есептеу

Электр энергиясын тұтынбай-ақ, бағдарламалық қамтамасыз етуді әзірлеу кезінде электр энергиясына жұмсалатын шығындарды есептеу мәні бар.

5.1-кестеге сәйкес бағдарламалық өнімді әзірлеу үшін 218 сағат қажет. Енді 218 сағат ішінде жұмсалатын электр энергиясының құнын есептеу қажет. Принтер үшін есептеу 16 сағат кезеңі үшін жүргізіледі, себебі принтерді үнемі пайдалану қажет емес.

$$Э = З_{эл.эн.обор.} + З_{доп.нужды.}, \quad (5.2)$$

Мұндағы:

$З_{эл.эн.обор.}$- жабдықтың электр энергиясына арналған шығындар;

$З_{доп.нужды.}$- қосымша мұқтаждықтарға электр энергиясының шығындары.

Жабдық үшін қажетті электр энергиясын есептеу мынадай формула бойынша анықталады:

$$З_{эл.эн.обор.} = \sum \boldsymbol{W} * К_{исц} * \boldsymbol{S} * \boldsymbol{T}, \quad (5.3)$$

Мұндағы:

W – тұтынылатын қуат, Вт;

$К_{исц}$ – пайдалану коэффициенті ($К_{ис}$ = 0,7..0,9);

Т – жұмыс уақыты;

S – тариф (1кВт / сағ = 23,81 тг).

Электр энергиясының құнын есептеу бойынша қорытынды 5.4-кестеде көрсетілген.

Кесте 5.4 – электр энергиясына шығындар

Құрылғы атауы	Төлқұжат бойынша қуат, кВт	Қуат коэффициенті	Құрылғының жұмыс уақыты, ч	ЭЭ бағасы тг/кВтч	Сомма, тг.
Ноутбук	0,8	0,7	218	23,85	2850,57
Принтер	0,6	0,9	16	23,85	206,06
Кондиционер	0,9	0,9	140	23,85	2704,6
Жарықтандыру	0,35	0,7	218	23,85	1273,83
Қорытынды:					7035,06

$$З_{эл.эн.обор.} = 7035,06(\text{тенге})$$

Қосымша қажеттіліктерге шығыстар электр энергиясына арналған шығыстардың 5% көлемінде жоғары көрсеткіш негізінде есептеледі:

$$З_{доп.нужды} = 5\% * З_{эл.эн.обор.}, \quad (5.4)$$

формулаға сәйкес қосымша қажеттіліктерге жұмсалатын шығындарды анықтаймыз: (5.4):

$$З_{доп.нужды} = 0.05 * 7035,06 = 351,753 \text{ (тенге)}$$

Барлық есептеулерге сүйене отырып, электр энергиясына толық шығындар құрайды:

$$Э = 351,753 + 7035,06 = 7386,795 \text{ (тенге)}$$

5.5 Еңбекақы төлеу шығындарын есептеу

Бағдарламалық қамтамасыз етуді әзірлеу үшін бұрын көрсетілгендей, үш қызметкер қажет.:

– жоба жетекшісі-жұмыс уақытын басқару, жұмыс процестерін түзету, үйлестіру, пәндік облысты зерттеу;

– әзірлеуші-БӨ әзірлеу, тестілеу және сүйемелдеу.

– аппараттық криптография- хабарламаны шифрлеу және дешифрлеу.

Еңбекақы төлеу шығындарының сомасын келесі формула бойынша есептеуге болады:

$$З_{тр} = \sum ЧС_i * T_i \quad (5.5)$$

Мұндағы:

$ЧС_i$ – і қызметкердің сағаттық мөлшерлемесі, тг;

T_i – модельді әзірлеудің еңбек сыйымдылығы, адам×сағ; і-қызметкердің санаты

n – БӨ әзірлеумен айналысатын қызметкерлердің саны.

Жұмыс уақыты әр түрлі, сондықтан әрбір қызметкердің сағаттық мөлшерлемесін және жалпы жалақы көлемін белгілеу мағынасы бар.

Қызметкердің сағаттық мөлшерлемесін мынадай формула бойынша есептеуге болады:

$$ЧС_i = \frac{ЗП_i}{ФРВ_i} \quad (5.6)$$

Мұндағы:

$ЗП_i$ – і-ші қызметкердің айлығы, тг;

$ФРВ_i$ – і жұмыс уақытының айлық қоры, сағат.

Басшының айлық жалақысы 220 000 теңгеге тең және әзірлеушінің айлық жалақысы 200 000 теңгеге тең. (4.6):

$$ЧС_{руководитель} = \frac{220\,000}{21 * 8} = 1\,309,5 \text{ тг/ч}$$

$$ЧС_{разработчик} = \frac{200\,000}{21 * 8} = 1\,190,5 \text{ тг/ч}$$

Басшының сағаттық мөлшерлемесі 1 309,5 (тг/сағ) құрайды, әзірлеудің еңбек сыйымдылығы 102 сағатқа тең. Әзірлеушінің сағаттық мөлшерлемесі 1 190,5 (тг/сағ) құрайды, әзірлеудің еңбек сыйымдылығы 218 сағатқа тең. (5.5) формулаға сәйкес қызметкерлердің еңбекақысына арналған шығындар сомасын есептеуге болады:

$$З_{тр} = 1\,309{,}5 * 102 + 1\,190{,}5 * 218 = 133\,569 + 259\,529 = 393\,098$$

Еңбек ақы төлеу бойынша шығындарды есептеу (5.5) кестеде көрсетілген.

Кесте 5.5 – Жалақыны есептеу

Жұмысшы санаты	Біліктілігі	БӨ әзірлеудің еңбек сыйымдылығы, час.	Сағаттық мөлшерлеме, тг/ч	Сомма, тг.
Басшы	Жобалаушы-инженер	102	1 309,5	133 569
Әзірлеуші	Программист	218	1190,5	259 529
Қорытынды				393098

5.6 Әлеуметтік салық бойынша шығындарды есептеу

Қазақстан Республикасының Салық кодексіне сәйкес әлеуметтік салық еңбекақы төлеу қорының 9,5% - ын құрайды. Әлеуметтік салықты келесі формула бойынша есептеуге болады:

$$С_н = (ФОТ - ПО) * 0{,}095 \qquad (5.7)$$

Бұл жерде ПО зейнетақы қорына аударымдар ФОТ-тың 10% құрайды.

$$ПО = 393\,098 * 0{,}1 = 39\,309{,}8 \text{ тенге}$$

$$С_н = (393\,098 - 39\,309{,}8) * 0{,}095 = 33\,609{,}9 \text{ тенге}$$

Есептеу нәтижелері кестеде берілген (5.6):

5.6 кесте – әлеуметтік салықты есептеу

Жұмысшы санаты	Адам саны	Еңбек ақысы, тг	Зейнетақы аударымдары, тг	Әлеуметтік салық, тг
Басшы	1	133 569	13 356,9	11 420,14
Әзірлеуші	1	259 529	25 952,9	22 189,7
Қорытынды				33 609,9

5.7 Негізгі қорлардың амортизациясы

НҚ амортизация нормаларын салық кодексіне сәйкес анықтау қажет. НҚ амортизациясын келесі формула бойынша анықтауға болады:

$$A_г = \frac{С_{об} * Н_а}{100} \quad (5.8)$$

Мұндағы:

$С_{об}$ – жабдықтың құны;

$Н_а$-амортизация нормасы (амортизация нормасы = 25);

(5.8) формула ноутбук үшін бір жыл ішінде амортизациялық аударымдар үшін қажетті соманы есептеуге мүмкіндік береді:

$$A_г = \frac{343\,000 * 25}{100} = 85\,750 \text{ теңге}$$

Енді әзірлеу кезеңі үшін амортизация нормасын есептеу қажет:

$$A_г = \frac{85\,750 * 28}{365} = 6\,578{,}08 \text{ теңге}$$

Осылайша, барлық жабдық үшін амортизация нормасын есептеу қажет. Есептеу нәтижелері кестеде келтірілген (5.7).

Кесте 5.7 – НҚ амортизациясы

Құрылғы атауы	Құрылғының құны, тг	Жылдық амортизация нормасы,%	Жылдық амортизация суммасы, тг	Әзірлеудегі амортизация нормасы, тг
Ноутбук	343 000	25	85 750	6 578,08
Принтер	35 000	15	5 250	402,7
Модем	10 000	20	2000	153,4
Қорытынды:			93 000	7 314,18

БӨ әзірлеуге арналған шығыстар сметасы.

Барлық берілген есеп-қисаптардың негізінде (5.8) кестеде келтірілген нысан бойынша әзірлеуге арналған шығыстар сметасын ресімдеу қажет.

Кесте 5.8 – БӨ әзірлеу бойынша шығындар сметасы

Шығындар баптары	Сумма, тг
Жабдыққа арналған шығында	393 740

5.8 кестенің жалғасы

Электр энергиясына арналған шығындар	7386,795
Еңбекақы төлеу шығындары	393 098
Әлеуметтік салықтар	33 609,9
Негізгі қорлардың амортизациясы	7 314,18
Смета бойынша қорытынды:	835 148,875

5.8 БӨ ықтимал (шарттық) бағасын анықтау

БӨ-нің ықтимал (шарттық) бағасының құны тапсырыс берушінің (тұтынушының) және орындаушының экономикалық мүдделерін қанағаттандыратын деңгейде тиімділікті, сапаны және оны орындау мерзімін ескере отырып белгіленуі керек.

Қолданылатын БӨ үшін келісім-шарттық бағасы ($Ц_д$) келесі формула бойынша есептеледі:

$$Цд = Знир(1+Р/100) \quad (5.9)$$

Мұндағы:

$З_{нир}$ – БӨ әзірлеуге кеткен шығын (8.8 кестеден белгілі), тг;

Р – БӨ рентабельділігінің орташа деңгейі,% (20-30% мөлшерінде қабылданады). Бұл параметр 25% деп есептеледі.

$$Цд = 835\ 148{,}875 + 835\ 148{,}875 * 0{,}25 = 835\ 148{,}875 + 208\ 787{,}21875 = 1\ 043\ 936{,}09375 \text{ тенге.}$$

Бұдан әрі қосылған құн салығын (ҚҚС) есепке ала отырып, өткізу құнын анықтау қажет, ҚҚС ставкасы ҚР заңнамалық Салық кодексімен белгіленеді. 2019 жылға ҚҚС ставкасы 12% мөлшерінде белгіленген.

Іске асыру құны ҚҚС-ты ескере отырып есептеуге болады мынадай формула бойынша:

$$Ц_р = Ц_д + Ц_д * НДС, \quad (5.10)$$

$$Ц_р = 1\ 043\ 936{,}09375 + 1\ 043\ 936{,}09375 * 0{,}12 = 1\ 043\ 936{,}09375 + 125\ 272{,}33125 = 1\ 169\ 208{,}425 \text{ тенге}$$

5.9 БӨ жұмысының әлеуметтік-экономикалық нәтижелерін бағалау

Әзірлеушілердің экономикалық тиімділігі жобаны іске асырумен айналысатын жеке әзірлеушілердің де, компанияның да қаржылық жағдайын жақсарту болып табылады.

Бұл өнімді іске асыру барысында осы өнімнің техникалық-экономикалық негіздемесі мен тиімділігі туралы сұраққа жауап беруі тиіс плата нарығы, маркетинг және жарнама сияқты сұрақтарға жауап қарастырылып және алдағы уақытта шешілуі қажет.. Егер бұл өнім табысты іске асырылса, девелопер 259 529 теңге көлемінде жалақы алады. Егер бұл жоба үлкен инвестицияларға әкелетін болса, онда жоба ұзақ уақыт бойы өтеу мерзіміне жетеді.

Бұл жобаның құны 835 148,875 теңге, пайда 208 787,21875 теңгені құрады. Қорытындылай келе, бұл жобаның мүмкін бағасы 1 169 208,425 теңгені құрайды.

Қорытынды

Деректер қоры кез келген басқа ақпараттық жүйе сияқты әр түрлі қауіптерге ұшырайды. Ол – құпиялылықтың, тұтастықтың, қолжетімділіктің бұзылуы. Бірақ басқа деректер қорының көптеген жүйелеріне қарағанда, SQL сұраныстарының спецификалық тіліне байланысты аз қорғалған, ол деректер қорын тікелей қолданғанда үлкен мүмкіндіктер береді. Стандартты қорғаныс құралдары көбінесе бірқатар қауіп-қатерлерді жеңе алмайды, ал осы осалдықтарды жоюға арналған арнайы өнімдер өте аз. Негізгі нәтиже – шығу көп пайдаланушы режимде деректер қорымен жұмыс істеу және жұмыс істеу үшін мамандандырылған клиенттік қосымшаларды пайдалану болып табылады.

Басқа қажетті шара – деректер қорымен жұмыс істеу үшін ДҚБЖ мен операциялық жүйені мұқият баптау.

Көптеген пайдаланылатын ДБЖ-да қоғамдық игілікке айналатын барлық жаңа және жаңа осалдықтар кезең-кезеңімен анықталады және көптеген осы "дырамдарды" пайдаланады. Бұған жауап ретінде дайындаушы фирмалар осы осалдықтарды жойып, көптеген жаңартуларды шығарады.

Көптеген мәселелер, ақаулықтар, қателер пайдаланушылардың дұрыс жұмыс істемеуінен немесе қате күйге келтіруден немесе ДҚБЖ орнатудан немесе жүйенің қандай да бір басқа компоненттерін орнатудан туындайды. Сондықтан көптеген жағдайларда дұрыс және қауіпсіз жұмыс істеу үшін жүйені дұрыс баптау және сенімді қауіпсіздік саясатын жасау және пайдаланушыларға қолжетімділікті шектеу жеткілікті, бұл жүйенің қауіпсіздік әкімшісі үшін аса күрделі міндет болып табылмайды.

Ақпаратты қорғаудың бірде-бір компьютерлік жүйесі мүлдем қауіпсіз емес. Алайда қорғаудың барабар шаралары жүйеге қолжетімділікті едәуір қиындатады және қаскүнем күш-жігерінің тиімділігін төмендетеді (жүйені қорғауды бұзуға орташа шығындардың және күтілетін нәтижелердің қатынасы), жүйеге ену орынсыз болады. Қауіпсіздік жүйесіндегі негізгі элемент жүйе әкімшісі болып табылады. Сіз қандай құралдар сатып алсаңыз да, қорғау сапасы осы адамның қабілеттері мен күш-жігеріне байланысты болады.

Әдебиеттер тізімі

1 Баранчиков А.И., Баранчиков П.А., Пылькин А.Н. Алгоритмы и модели доступа к записям БД. -М.: Горячая линия-Телеком, 2011. 182 с.

2 Поляков А.М. Безопасность Oracle глазами аудитора: нападение и защита. М.: ДМК Пресс, 2014. 336 с.

3 Смирнов С.Н. Безопасность систем баз данных. М.: Гелиос АРВ, 2007. 352 с.

4 Кузнецов С.Д. Базы данных: учебник для студ. М.: Академия, 2012. 496 с.

5 Полтавцева М.А., Зегжда Д.П., Супрун А.Ф. Безопасность баз данных: учеб. пособие. –СПб.: Изд-во СПбПУ, 2015. 125 с.

6 Агальцов, В.П. Базы данных. В 2-х т.Т. 1. Локальные базы данных: Учебник / В.П. Агальцов. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. - 352 с.

7 Голицына, О.Л. Базы данных: Учебное пособие / О.Л. Голицына, Н.В. Максимов, И.И. Попов. - М.: Форум, 2012. - 400 с.

8 В. В., Погонышева Д. А., Степченко И. Г.. Безопасность информационных систем. Учебное пособие. — М.: Флинта, Наука, 2015. — 184 с.

9 Зрюмов Е. А. Базы данных для инженеров : учебное пособие / Е. А. Зрюмов, А. Г. Зрюмова; Алт. гос. техн. ун-т им. И. И. Ползунова. – Барнаул : Изд-во АлтГТУ, 2010. – 131 с.

10 Кириллов, В.В. Введение в реляционные базы данных.Введение в реляционные базы данных / В.В. Кириллов, Г.Ю. Громов. - СПб.: БХВ-Петербург, 2012. - 464 с.

11 Кудрявцева Р.Т. Теория информационной безопасности и методология защиты информации. Лекции. — Уфа: УГАТУ, 2012.

12 Максимов, Н.В. Современные информационные технологии: Учебное пособие / Н.В. Максимов, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2013. - 512 с.

13 Д. А. Организация и обеспечение безопасности информационно-технологических сетей и систем. - М.: КДУ, 2015. — 598 с.

14 Ржеуцкая С.Ю. Базы данных. Язык SQL: учеб. пособие / СЮ. Ржеуцкая. - Вологда: ВоГТУ, 2010. - 159 с.

15 В. Ф. Информационная безопасность и защита информации. — М.: ДМК Пресс, 2014. 702 с.

16 Официальный сайт первого в России независимого информационно-аналитический центра [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/malware

17 Securelist – все об интеренет-безопасности [Электронный ресурс]. – Режим доступа: https://securelist.ru/analysis/ksb/24580/kaspersky-security-bulletin-2014-osnovnaya-statistika-za-2014-god/

18 http://lab.infosec.uz/explore/c6

19 Подробнее: https://www.securitylab.ru/analytics/485977.php

20 https://go.microsoft.com/fwlink/?linkid=2043154
21 https://www.microsoft.com/ru-ru/sql-server/sql-server-editions-express
22 Громов В.И., Васильев Г.А. Энциклопедия безопасности-3 (с изменениями и дополнениями). Москва, 2000.
23 Обеспечение безопасности при работе с ПЭВМ Маньков В.Д. НиТ 2005
24 Вербовецкий А.А. Основы компьютерных технологий и современные ПК. - М.: АЛЕКС, 2002. - 264 с.
25 Жигарев А.Н., Макарова Н.В., Путинцева М.А. Основы компьютерной грамоты. 1987.
26 Михаил Кутузов, Андрей Преображенский Выбор и модернизация компьютера, 2004