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: «Кәсіпорынның ақпараттық жүйелеріне жасалатын шабуылдарды анықтау жүйесінің модулін әзірлеу»
Мамандығы: 5В100200 – «Ақпараттық қауіпсіздік жүйелері»
Орындаған: Утарғалиева Әсел Тобы: СИБк-15-1
Ғылыми жетекші: с.ғ.к., доцент Бердібаев Р. Ш.

Кеңесшілер:
Экономикалық бөлім бойынша:
э.ғ.к., профессор Әрекбаева Қ.Г.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «13» 05 2019 ж.
(қолы)

Тіршілік қауіпсіздігі бөлімі бойынша:
аға оқытушы Торғаев Д.Д
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «27» 05 2019 ж.
(қолы)

Есептеу техникасын қолдану бойынша:
с.ғ.к., доцент Бердібаев Р.Ш.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «31» 05 2019 ж.
(қолы)

Мөлшер бақылаушы:
аға оқытушы, т.ғ.м. Аскарова Н.Б
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «03» 06 2019 ж.
(қолы)

Пікір беруші:
_____
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «_____» _____ 201__ 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: Ұтарғалиева Әсел Қуанышкереевна
(аты-жөні)

Жобаның тақырыбы: Кәсіпорынның ақпараттық жүйелеріне қасалған шабуылдарды анықтау жүйесінің модулін әзірлеу.

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

Аяқталған жұмысты тапсыру мерзімі: «31» қаңтар 2019 ж.

Жобаға алғашқы деректер (талап етілетін зерттеу (жоба) нәтижелерінің параметрлері және зерттеу нысанының алғашқы деректері): Кәсіпорынның ақпараттық жүйелеріне қасалған шабуылдарды анықтау модулін әзірлеу. Басқа кіруді келесі қасалған шабуылды анықтап, ол туралы сайт иесіне хабарлау.

Диплом жобасындағы әзірленуі тиіс мәселелер тізімі немесе диплом жобасының қысқаша мазмұны: Кәсіпорынның сайтына қасалған шабуылдарды, әзірленген модуль келізінде тексеріп, администраторға есептеу. Пайдаланушы жіберген сұранысты қасалған ерене келізінде тексеріп, одан сәйкес келмейтін сұранысты қалыпты қалыпқа келтіріп және шабуылдаушыға бұғаттау.

Графикалық материалдардың (міндетті түрде дайындалатын сызбаларды көрсету) тізімі: 1. Рұқсат сөз басқа кіруді анықтау жүйесінің түрлері.
2. Басқа кіруді анықтау жүйесінің негізгі құрылғылары.
3. Python бағдарламалау тілі.
4. Кәсіпорын сайтына қасылған шабуылдар
5. Модельдің жүйелік жасау принципі.

Негізгі ұсынылатын әдебиеттер: 1 Лукацкий А.В. Обнаружение вторжений. - СПб.: БХВ-Петербург, 2007.
2 Милославская Н.Г., Толстой А.И. Интрасети: Обнаружение вторжений. - М.: Юнити, 2001.
3. Акбарова Ш.А., Таңшев А.А. Классификация IDS // «Молодой ученый» № 15 (149), сәуір 2017.
4. Бекишева А.И. Методические указания к выполнению экономической части дипломной работы для бакалавров специальности 5В0703 - Информационные системы.

Жоба бойынша жобаның бөлімдеріне қатысты белгіленген кеңесшілер

| Бөлімдері | Кеңесшілері | Мерзімі | Қолы |
|---|---|---|---|
| Есептеу техникасы б-і | Серікбаев Р.Ш. | 21.01-15.05.19 | |
| Экономика бөлімі | Ахметбаева Ж.Г. | 04.03-13.05.19 | |
| Өндірістік қауіпсіздік бөлімі | Тұзақов Д.Д. | 13.05-27.05 | |
| | | | |
| | | | |
| | | | |
| | | | |

Диплом жобасын дайындау
КЕСТЕСІ

| Бөлімдердің атауы, әзірленетін мәселелердің тізімі | Ғылыми жетекшіге ұсыну мерзімдері | Ескерту |
|---|---|---|
| Кіріспе | 21. 01. 2019 | |
| Ақпараттың жүйелерге жасалатын шабуылдар түрлері | 04. 02. 2019 | |
| IDS түрлері және басқа құралдарды анықтау жүйелерінің түрлері | 18. 02. 2019 | |
| Шабуылдарды анықтау жүйелерінің жіктелуі. | 04. 03. 2019 | |
| Шабуылдарды анықтау технологиясы | 17. 03. 2019 | |
| Шабуылдарға қарсы әрекет ету жүйелері | 02. 04. 2019 | |
| Python бағдарламалау тілі | 11. 04. 2019 | |
| Веб-қосымшаларға арналған Django фреймворкі | 13. 04. 2019 | |
| bypass waf шабуылдары | 15. 04. 2019 | |
| Қазіргі сайттағы жасалған шабуылдар және олардың анықтау жүйесінің моделі | 17. 04. 2019 | |
| Техникалық экономикалық негіздеме | 18. 04. 2019 | |
| Өмір тіршілік қауіпсіздігі | 15. 05. 2019 | |
| Қорытынды. | 31. 05. 2019 | |

Тапсырманың берілген уақыты « 28 » қаңтар 2019 ж.

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

Жобаның
ғылыми жетекшісі _____ (Бердібаев Р. Ә.)
(қолы) (аты-жөні)

Орындалатын тапсырманы
қабылдаған студент _____ (Ұлғалымова Д. Қ.)
(қолы) (аты-жөні)

## АҢДАТПА

Бұл дипломдық жобада «Trassir» компаниясының сайтына жасалатын шабуылдарды анықтау жүйесінің модулі әзірленді. Бұл модульдің артықшылығы рұқсатсыз басып кірулерді анықтап, оны дер кезінде сайт иесіне ескерту және шабуылдаушыны бұғаттау болып табылады.

Экономикалық бөлімде қажетті жабдықтар мен бағдарламалық қамтамасыз етуге қажетті экономикалық шығындардың есебі көрсетілді.

Өмір тіршілік қауіпсіздігі бөлімінде компьютермен жұмыс кезінде бөлінетін сәулелердің адам ағзасына әсері, олардан қорғану іс-шаралары және элетро-магниттік өріс әсерінен қорғану жолдары қарастырылды.



## АННОТАЦИЯ

В данном дипломном проекте разработан модуль системы обнаружения атак на сайте компании «Trassir». Преимуществом этого модуля является обнаружение вторжений, своевременное предупреждение владельца сайта и блокирование атакующего.

В экономической части показан расчет экономических затрат на необходимое оборудование и программное обеспечение.

В разделе безопасность жизнедеятельности рассмотрены влияние выделяющихся в работе с компьютером излучений на организм человека, меры защиты от них и способы защиты от воздействия электромагнитных полей.



## ANNOTATION

In this thesis project we have developed a module system for the detection of attacks on the website of the company «Trassir». The advantage of this module is the detection of unauthorized intrusions, timely warning of the site owner and blocking the attacker.

The economic part shows the calculation of economic costs for the necessary equipment and software.

In the section life safety the influence of radiations released in the work with the computer on the human body, protection measures against them and methods of protection from the effects of electromagnetic fields are considered.

**Мазмұны**

# Кіріспе

Маңызды құндылықтар ұрлықтан және жоюдан қорғалуы тиіс. Қазіргі таңда барлық дерлік мекеме орындарында ұрыларға қарсы, олар туралы құқық қорғау органдарына хабарлайтын, тіпті орын алған өрт туралы ескертетін дабыл құрылғылары орнатылған. Бұл ғимараттардың тұтастығын және оның қауіпсіздігін қамтамасыз ету үшін қажетті шаралар.

Сонымен қатар, компьютерлік жүйелер мен деректердің де осындай тұтастығы мен қауіпсіздігін қамтамасыз еткен жөн. Бүгінде интернет дербес ақпараттан бастап қаржылық ақпаратқа дейін кез келген деректің жіберілуіне мүмкіндік жасайды. Сонымен бірге, ол көптеген қауіп тудырады. Қаскүнем қолданушылар мен хакерлер пайда іздеу мақсатында - уақытылы ретке келтірілмеген жүйелерді, троянды конь деп аталатын вирусы бар жүйелерді және қауіпті қызмет істейтін желілерді – іздейді. Администраторлар мен қауіпсіздік жөніндегі топ мүшелері хакерлік бұзушылықтарды лезде анықтап, оған уақытылы қарсы тұруы үшін, оларға дабыл жүйелері қажет. Хакерлік кіру жүйесін анықтау осындай ескерту жүйесі болып табылады.

Рұқсатсыз кіруді анықтау жүйесі – бұл жұмыс станциясына немесе компьютерлік желіге авторизацияланбаған кіруді анықтауға арналған бағдарламалық немесе аппараттық кешен. Кәсіби ортада IDS аббревиатурасы (ағылш. Intrusion Detection System-басып кіруді анықтау жүйесі) кеңінен қолданылады. IDS-жүйелер осал сервистерге және пайдаланушыларды есепке алу/бақылау жүйелеріне жасалған желілік шабуылдар, жергілікті компьютер немесе желі файлдарына қол жеткізу, сондай-ақ зиянды бағдарламалық қамтамасыз ету (вирустар, трояндар, құрттар) белсенділігі сияқты авторизацияланбаған кірудің әрекет түрлерін анықтауға мүмкіндік береді.

Басып кіруді анықтау жүйелері бүгінгі күні корпоративтік ақпараттық жүйелер мен компьютерлік желілерде кеңінен таралған. Компьютерлік желілер мен ақпараттық жүйелерге басып кіруді анықтау ғылыми зерттеулердің жаңа бағыты емес. Сонымен қатар Cisco және Network Associates сияқты бірнеше үлкен бәсекелестері бар жақсы игерілген коммерциялық аймақ. Жалпы ақпараттар бойынша, белгілі рұқстасыз кіруді анықтау жүйелері көп жағдайда қате іске қосылады және компаниялардың ақпараттық ресурстарына жасалған барлық шабуылдарды таппайды. Бұл тұрғыда рұқсатсыз кіруді анықтау жүйесін әзірлеу антивирустық бағдарламалық қамтамасыз ету саласындағы соңғы үрдістерге ұқсас. Антивирустық бағдарламалық қамтамасыз етудің бұрынғы нұсқалары, сондай-ақ жаңа файлдарды құрған сайын пайдаланушыны мазалады. Алайда, соңғы бірнеше жылда антивирустық бағдарламалық қамтамасыз ету айтарлықтай жетілдірілген. Енді пайдаланушылар антивирустық бағдарламалық қамтамасыз етудің олардың компьютерінде орындайтын әрекеттеріне назар аудармайды. Бұл ретте олардың көпшілігі барлық белгілі вирустарды анықтайтынына сенімді.

Рұқсатсыз кіруді анықтау жүйесін құру тұжырымдамасы бастапқыда 1980 жылы Джеймс Андерсон ұсынды. Алайда, бұл ғылыми бағыт 1987 жылға дейін дерлік Дороти Деннинг басып кіруді анықтау моделін жариялағанға дейін зерттелмей қалды. 1988 жылы рұқсатсыз кіруді анықтау жүйесінің кем дегенде үш прототипі болды. Келесі жылдары прототиптердің саны үнемі өсіп отырды. Көптеген елдердің үкіметтері, олардың компьютерлік жүйелері жеткіліксіз қорғалғанын түсіне отырып, рұқсатсыз кіруді анықтау жүйесін құру саласындағы зерттеулер үшін қаржы бөлді. Соңғы жылдарда басып кіруді анықтау жүйесін зерттеуге бірнеші миллиардтаған доллар жұмсалған.

Рұқсатсыз басып кіруді анықтау кемелденген технологияға және өнеркәсіптік мүдделердің саласына айналғаннан кейін барлық қарапайым проблемалар сәтті шешілді. Соңғы уақытта бұл салада айтарлықтай серпінді шешімдер табылған жоқ. Оның орнына, ұқсас жүйелерді әзірлеушілер негізінен белгілі рұқсатсыз басып кіруді анықтау әдістерін жетілдіреді. Осыған байланысты, осы саладағы дәстүрлі зерттеу бағыттары аз мәнге ие болады. Сондықтан, болашақ рұқсатсыз басып кіруді анықтау бойынша зерттеулер, болжанып отырғандай, салыстырмалы түрде төмендегі зерттелмеген салаларды қарастырады:

- шабуылға жауап беру механизмдері;
- рұқсатсыз басып кіруді анықтау таралған жүйелерінің архитектурасы;
- рұқсатсыз басып кіруді анықтау кезінде жүйе компоненттерінің өзара әрекеттесу стандарттары;
- басып кіруді анықтаудың жаңа парадигмалары.

Соңғы уақытта пайдаланушылардың басып кіруді анықтау жүйелерін қолдануы белсенді түрде танымал болып келеді. IDS-әрбір пайдаланушыға қажетті ақпараттық қауіпсіздікті қамтамасыз ету барысындағы маңызды элемент. Рұқсатсыз кіруді анықтау жүйесі компьютерлік шабуылдарды анықтауға және оны бұғаттауға ғана емес, сонымен қатар ыңғайлы графикалық интерфейсте орындауға да мүмкіндік береді — пайдаланушыдан желілік хаттамалар мен ықтимал осалдықтар туралы арнайы білім талап етілмейді.

# 1 Техникалық бөлім

## 1.1 Ақпараттық жүйелерге жасалатын шабуылдар түрлері

Шабуыл – бұл ақпараттық жүйеге (АЖ) басып кіру үшін пайдаланылатын қандай да бір осалдықты пайдаланудың нақты тәсілі. Шабуылдар АЖ (сервер, желілік жабдық және т.б.) элементтерін конфигурациялау (баптау) қателерін, сондай-ақ операциялық жүйелерді жобалау, қызметтер мен қосымшалардың өзара іс-қимыл және бағдарламалық қамтамасыз ету хаттамаларын әзірлеу кезінде жіберілген тұжырымдамалық қателерді қоса алғанда іске асыру қателерін сәтті пайдалана алады.

Әдетте, ақпараттық жүйеге рұқсатсыз басып кіру екі кезеңнен тұрады. Бірінші кезеңде объектіде қандай да бір осалдықтардың болуын анықтауға мүмкіндік беретін шабуыл объектісі туралы ақпарат жинау жүргізіледі (пайдаланылатын операциялық жүйенің түрі, желілік мекен-жайлар, қолжетімді желілік сервистер және т.б.). Екінші кезең-шабуылды іске асыру процесі. Шабуылдың соңғы мақсаты ақпараттық жүйеде сақталатын, өңделетін және берілетін ақпараттың тұтастығын, құпиялылығын немесе қол жетімділігін бұзу болып табылады. Пайдаланылатын осалдықтың деңгейіне байланысты барлық шабуылдарды торап деңгейінің шабуылы және желі деңгейінің шабуылы деп екіге бөлуге болады [1].

Біріншісі концептуалды осалдықтар мен қолданбалы хаттамаларды (SMTP, DNS, SNMP және т.б.), операциялық жүйелер мен бағдарламалық қамтамасыз ету компоненттерінің іске асыру қателіктерін пайдаланады. Желі деңгейінің шабуылдары ашық жүйелердің өзара іс-қимыл моделінің арналық, желілік және транспорттық деңгейлеріне сәйкес келетін хаттамалардың концептуалды осалдықтарын пайдаланады.

## 1.2 Басып кіруді анықтау процесінің моделі және шабуылдарды анықтау әдістері

Жалпы түрде шабуылдарды анықтау процесінде рұқсатсыз басып кіруді анықтау жүйесімен жүзеге асырылатын функциялар жиынтығы бастапқы деректерді жинағын, оларды бастапқы өңдеуді, талдауды, қорытуды және сақтауды, анықталған бұзушылықтар бойынша реакцияны қоюды қамтиды.

Бастапқы деректерді жинау барысында ақпараттық жүйелердің жұмыс істеу процесі туралы ақпарат алу жүргізіледі. Содан кейін берілген деректерді болдырмау және талдау үшін жарамды құрылымдалған түрдегі ақпараттық жүйелер жағдайы туралы ақпаратты ұсыну мақсатында берілген ақпаратты бастапқы өңдеу жүзеге асырылады. Келесі кезеңде деректер белгілі бір математикалық модельдер мен әдістер негізінде талданады, бұл ретте шабуылдарды анықтау мақсатында ақпараттық жүйелер жағдайы туралы ақпаратты одан әрі өңдеу жүргізіледі. Жинау, алғашқы өңдеу және талдау

операциялары көптеген деректерді өңдеуді талап етеді. Рұқсатсыз басып кіру процесінің тиімділігіне әсер ететін маңызды сипаттамалардың бірі көрсетілген операциялар орындалатын жиілік болып табылады. Деректерді сақтау функциясы басып кіруді анықтау және талдау үшін қажетті ақпаратты жинақтау жүйелерінің жұмысын хаттамалауды қамтамасыз етуге арналған. Шабуылдар анықталған жағдайда, басып кіруді анықтау жүйесі шабуылдардың дамуын бұғаттау үшін қарсы өлшемдерді әзірлеу бойынша шешім қабылдауды жүзеге асырады.

Ақпараттық жүйелердің жағдайы туралы деректерді жинау барысында пайдаланылатын ақпарат көздері ретінде операциялық жүйенің аудит журналдары және қосымшалар, жүйелік ресурстардың жағдайы және желілік трафик пайдаланылады.

Операциялық жүйелер аудит журналдары олардың жұмыс істеу процесінде пайда болатын оқиғалар туралы жазбаларды қамтиды. Журналдарға енгізілетін жазбалардың құрылымы мен типтері операциялық жүйелермен анықталады, бірақ олар міндетті түрде оқиға уақыты, оқиға көзінің идентификаторы және әрекет түрі туралы мәліметтерді қамтиды. Аудит журналдарында драйверлер мен қолданбалы бағдарламаларды жүктеу, түсіру және олардың жұмысындағы іркілістерді қамтитын ақпараттың кең спектрі; пайдаланушылардың есептік жазбаларын басқару және пайдалану, файлдардан, директориялар мен құрылғылардан бастап және операциялық жүйенің ішкі объектілерімен (семафорлар, сипаттамалар және т.б.) аяқтай отырып, Операциялық жүйе объектілеріне қол жеткізу бар. Қосымшалардың журналдары файлдық жүйе объектілеріне жүгінген кездегі оқиғалар туралы ақпаратты, желілік сервистер мен қол жеткізу әрекеттері туралы ақпаратты тіркейді.

Жүйелік ресурстардың жай-күйі туралы ақпарат операциялық жүйелердің жұмыс қабілеттілігін сипаттайтын көрсеткіштердің мәні болып табылады: процессорды жүктеу, физикалық және виртуалды жадыны пайдалану, қатты дискіге жүгіну жиілігі, енгізу-шығару процесінің қарқындылығы, орнатылған желілік қосылыстар және т.б. Берілген көрсеткіштердің мәндері шабуылдарды табу процесінде талдау үшін үлкен қызығушылық тудырады.

Желі трафигі ақпараттық жүйелердің байланыс арналары арқылы өтетін көптеген пакеттерді ұсынады. Желілік трафик ашық жүйелер сәйкестігі моделінің арналық (Ethernet 802.3 фреймдері), желілік (ARP, RARP, IP, ICMP пакеттер) және көліктік деңгейіне (TCP, UDP пакеттер) сай келетін пакеттерді өңдеу мақсатында декодтауға ұшырайды. Декодтау-бұл кіріс деректері, коммуникациялық хаттамалар пакеттерінің форматтарына сәйкес келетін құрылымдар бар жад аймағына салу. Желілік пакеттерді декодтау процесі жіберуші мен алушының мекен-жайы, әр түрлі жалаушалар мен коммуникациялық хаттамалардың сипаттамалары сияқты бірнеше бөлімдердің орындалуына негізделген. Жоғарырақ деңгейдегі хаттамалар (RPC, DNS, SMTP және т.б.) мен олардың бағдарламалық жүзеге

асыруларындағы осалдықты пайдаланатын шабуылдарды табу мақсатында, бастапқы декодтау процесі кеңейтілуі мүмкін. Деректерді жинау желілік құрылғыларда (коммутаторлар, маршрутизаторлар, көпірлер), желіаралық экрандарда немесе жұмыс станциялары мен серверлерінде (деректер базасының сервері, пошталық сервер және т.б.) орналастырылатын арнайы датчиктердің көмегімен жүргізіледі.

Бастапқы өңдеуден өткен соң, берілген деректер олардың корреляциясын және шабуылдардың болу белгілерін анықтайтын талдауға түседі. Талдау құралдары жұмыс істеу процесінде келесі ақпарат көздерін қолданады: алғашқы өңдеуден өткен деректер, талдаудың алдыңғы циклдерінің нәтижелері, білім базасынан алынған шабуыл белгілерін сипаттайтын мәліметтер, жүйенің қалыпты жұмыс істеу шаблондары және т. б.

Шабуыл анықталған жағдайда, рұқсатсыз басып кіруді анықтау жүйесі әрекет етеді, бұл талдау нәтижелерін ақпарат қауіпсіздігі қызметінің әкімшісіне немесе қызметкеріне ұсыну болып табылады. Барлық нәтижелер пайдаланушының графикалық интерфейсі бар басып кіруді анықтау жүйесін бірыңғай басқару консоліне ұсынылуы тиіс және персоналды хабарлаудың қосымша тәсілдері, мысалы, электрондық пошта, пейджер немесе хабарламалар қызметі қолданылуы тиіс.

Әрекет ету (реагирование) процесінде басып кіруді анықтау жүйесі ақпарат қауіпсіздігіне төндірілген қатер деңгейін бағалауға міндетті және қарсы өлшемдерді әзірлеу бойынша шешім қабылдауға тиіс. Рұқсатсыз басып кіруді анықтау жүйесінің құрамында қарсы өлшемдерді әзірлеу бойынша жүзеге асыратын (контрмер) компоненті болған жағдайда, шабуыл салдарын азайту мақсатында басып кіруді бұғаттау процесін автоматтандыруға болады. Әрекет ету нұсқасы ақпараттық жүйелерде қабылданған қауіпсіздік саясатына сәйкес болуы тиіс және мынадай іс-әрекеттерді қамти алады: шабуылданатын жұмыс орнын қайта конфигурациялау, қолданылатын сессияны жабу хаттамасына сәйкес келетін компрометирленген есептік жазбаларды бұғаттау.

Деректерді сақтау функцияларын іске асыру дегеніміз – анықталған оқиғалар туралы ақпаратты, аудит журналдарының көшірмелерін және білім базасында талдау үшін қажетті басқа да ақпаратты сақтауды. Білім базасы белгілі түрдегі шабуылдардың сипаттамасын, қалыпты мінез-құлықтың үлгілерін, анықталған күдікті оқиғалар туралы мәліметтерді қамтуы мүмкін. Білім базасында дабыл сигналының жасалуын негіздейтін егжей-тегжейлі ақпарат болуы тиіс. Білім базасын табысты жүргізу және басып кіруді анықтау жүйесіне көптеген деректерге қол жеткізуді қамтамасыз ету үшін, деректерді сақтау және қорғау саясаты болуы тиіс.

Жалпы түрде, таңдап алынған анықтау әдісіне қарамастан, басып кіруді анықтау үшін қажетті әрекеттер тізбегі келесідей. Бірінші кезеңде, ақпараттық жүйелердің жай-күйі туралы жиналған деректер (ұстап қалған желілік трафик, жүйелік ресурстар туралы ақпарат, жүйелік шақырулардың реттілігі туралы ақпарат) бастапқы өңделуге ұшырайды. Ақпаратты бастапқы өңдеудің

мақсаты шабуылдаушы әрекеттерін анықтау мәнін тікелей талдауға арналған белгілі бір түрде құрылымдалған деректер түрінде ақпараттық жүйелердің жағдайы туралы бастапқы деректерді ұсыну болып табылады. Деректерді ұсыну формалары мен тәсілдері талдау процесінде қолданылатын математикалық модельдер мен әдістер және операциялық жүйелердің ерекшеліктеріне байланысты болып келеді. Мысалы, Windows операциялық жүйесінде ұсталып қалған желілік пакеттер туралы ақпарат байт массивтері түрінде қалыптастырылып, ортақ жад тетігі арқылы талдау үшін ұсынила алады.

Көрсетілген нысандар мен тәсілдерді әзірлеу процесі итерациялық болып табылады. Ол басып кіруді анықтау жүйесін жобалаудың барлық кезеңдерінде жүзеге асырылады және, тікелей, бағдарламалық қамтамасыз етуді (ПО) әзірлеу кезінде аяқталады. Әрбір келесі итерация абстракцияның төменгі деңгейіндегі сипаттама болып табылады. Нәтижесінде шабуылдарды анықтаудың жеделдігіне сыни әсер ететін құрамдастардың бірі – құрылымдалған деректерді ұсынудың әзірленген нысандары мен тәсілдері болып табылатынын ерекше атап өткен жөн [2].

Жалпы түрде, шабуылды талдау және анықтау процесі екі кезеңнен тұрады: шабуылды анықтау және оны тану. Шабуылдарды анықтау – құрылымдалған деректерден шабуылдаушы әрекеттердің белгілерін іздеу процесі. Шабуылдарды тану – анықталған белгілердің негізінде белгілі бір типтердің басып кіруін анықтау жүйесіне жатқызу процесі. Шабуылдарды анықтау барысында және оны тану процесінде білім базасы қолданылады.

Білім базасын қалыптастыру кейбір оқыту деректер үлгісінің негізінде жүргізіледі. Білім базасындағы ақпараттың құрамы, нысаны және ұсыну тәсілдері (теріс пайдалану немесе аномалиялар) рұқсатсыз басып кіруді анықтау жүйесінде пайдаланылған табу тәсіліне байланысты әр түрлі болуы мүмкін. Мысалы, сигналатуралық әдісті пайдалану анықталған кезде білім базасында белгілі үлгідегі шабуыл сигналдарының деректер базасы болуы тиіс. Аномалияларды анықтаудың статистикалық әдістерін қолдану, ақпараттық жүйедегі қалыпты жұмыс істеу үлгілері туралы, статистикалық деректер базасын қалыптастыруды көздейді. Құрылымдалған мәліметтерді талдау үшін нейрондық желілер теориясының әдістерін қолданған жағдайда, білім қоры оқыту процесінде нейрондардың кірісінде алынған салмақ коэффициенттерінің жиынтығы болып табылады. Демек, білім базасын қалыптастыру тәсілін әзірлеу, оқыту үлгісінің мөлшері мен құрамын анықтау, сондай-ақ табу тәсілі мен әдісіне байланысты.

Шабуылдарды тану процесі оны белгілі бір үлгілерге жатқызумен немесе белгісіз түрдегі шабуылдың ақпаратық жүйелерге әсер етуін анықтаумен аяқталады. Соңғы жағдайда, бұдан әрі осындай шабуылдарды жіктеп отыру мақсатында, білім базасын кейіннен модификациялай отырып, ақпараттық жүйенің жұмыс істеу процесіне әсер етуін зерттеу жүргізіледі.

Жоғарыда қарастырылған іс-қимылдар тізбегі, шабуылдарды анықтау кезеңінде, басып кіруді анықтау жүйесінің жұмыс істеу процесін толық сипаттайды.

Бірнеше анықтау әдістері бар, олардың қолданылуы бірінші кезекте таңдалған табу тәсіліне байланысты.

Сигнатуралық талдау шабуылдарды анықтау процесін теріс пайдалануды анықтау процесі ретінде іске асыратын әдістердің бірі болып табылады. Сигнатурлық талдау белгілі шабуылды білім базасында сақталған сигнатурамен сиппатталуын қарастырады, сигнатура ретінде символдар жолы, арнайы тілдегі семантикалық өрнек, формальды математикалық модель және т.б. қолданылуы мүмкін.

Сигналатуралық әдістің мәні мынада: датчиктер арқылы жиналған, қорғалатын жүйедегі оқиғалар туралы бастапқы деректерде, мамандандырылған деректер базасында сақталатын, шабуылдар сигналдарын іздеу процесі орындалады. Бұл тәсілдің артықшылығы – шабуылдарды анықтаудың жоғары дәрежедегі дәлдігі, негізгі кемшілігі – сигналдар деректер базасындағы басып кіруді анықтау жүйесінде жоқ априорлы белгісіз шабуылдарды анықтау мүмкін еместігі.

Шабуылдарды анықтаудың сигналдық әдістерінің арасында контекстік іздеу әдісі кеңінен таралған, ол белгілі бір символдардың қорғалатын жүйесіндегі оқиғалар туралы бастапқы деректерде анықталған. Контекстік іздестірудің функционалдық мүмкіндіктерін кеңейту үшін, кейбір жағдайларда шабуыл сигналын сипаттайтын арнайы тілдер қолданылады.

Қазіргі уақытта кеңінен қолданылатын контекстік іздеу әдісін қолдану нұсқаларының бірі «аудит журналдарындағы іздерді талдау» деп аталады. Ақпарат қауіпсіздігіне қатысты жүйедегі кез келген оқиға журналда тиісті жазба түрінде көрсетілуі тиіс болғандықтан, әдістің мәні оқиғалардың жүйелік журналдарынан алынған ақпаратты шабуыл сигналдарымен салыстыру болып табылады. Шабуылдар сценарийлері оқиғалардың тізбектері түрінде немесе операциялық жүйелер оқиғалар журналдарында, қосымшаларда, маршрутизаторларда, желіаралық экрандарда, коммутаторларда және арнайы агенттерде (датчиктерде) іздеу жүргізілетін деректер үлгілері түрінде ұсынылуы мүмкін. Ақпарат қауіпсіздігі саясатының бұзылуын жылдам анықтау үшін, жүйелік журналдарды талдау нақты уақытқа жақын режимде жүргізіледі. Журналдарды талдауды қолдану аудит журналдарында жалпы жазба форматы болмаған жағдайда күрделі болып табылады.

Мәтіндік іздеу әдісін тиімді қолданудың тағы бір нұсқасы – желілік трафикті талдау негізінде шабуылдарды анықтау. Бұл әдіс бастапқы деректер ағымында анықталуы қажет шабуылдар сигнатурасының параметрлерін дәл анықтауға мүмкіндік береді. Айтылған әдіс коммуникациялық хаттамалардың дәл сипатталған пакеттері және фреймдері негізінде жүзеге асады.

Сигналдарды талдау әдісі шекті мәндерді пайдалана отырып немесе пайдаланбай қолданылуы мүмкін. Егер шекті мәндер анықталмаса, онда шабуыл сигналмен қарапайым сәйкес келу негізінде анықталады. Егер шекті

мән анықталса, онда оқиғалар сәйкес келуі немесе оқиғалар тізбегі сигналмен шектік мәннен асып кетсе, шабуыл анықталды деп есептеледі. Шекті мәндер пайыздар, жиілік және т.б. түрінде берілуі мүмкін.

Шабуылдарды анықтаудағы ең үлкен табыс – торап деңгейіндегі датчиктерді және желілік деңгейдегі датчиктерді құрамдастырып қолдану негізінде алынған ақпараттың сигналдық талдауын қамтамасыз етеді. Теріс пайдалануды анықтаудың сигналдық әдісінің негізгі кемшіліктері:

- жаңадан анықталған шабуылдардың сигналдарымен сигналдар білімдерінің базасын жиі жаңарту қажеттілігі;
- шабуыл сигналдарын өзгерту және қосу үшін тетіктерді іске асыру қажеттілігі;
- сигналдардың білім базасын ұлғайту кезінде талдау уақытын арттыру.

Теріс пайдаланулар анықталған кезде, жағдайларды талдау әдісі торап деңгейінің датчиктері жинайтын ақпаратты талдау үшін қолданылады. Шабуылдар сигнатурасы жүйенің жай-күйі мен олардың арасындағы өткелердің кезектілік диаграммасы ретінде ұсынылады. Шабуыл шаблонындағы жағдай мәні шынайы болуы тиіс түйреуіш өрнектер түрінде сипатталған белгілі бір оқиғалар бойынша ауысатын жүйенің жай-күйіне сәйкес келеді. Негізінен, жай-күйлерді талдау негізінде жасалған шабуылдар сигнатуралары соңғы автоматтар теориясына немесе Петри желілеріне негізделген математикалық модельдермен сипатталады.

Сараптама жүйелерінің әдістерін теріс пайдалануды анықтау үшін де, аномалияны анықтау үшін де кеңінен қолдануға болады. Сараптама жүйелерін қолдану деректердің екі түріне: фактілер мен ережелерге негізделген. Фактілер – НЖ жұмысы туралы бастапқы деректер, ал келіп түскен фактілер жиынтығы негізінде шабуыл жасау туралы логикалық шешімдердің алгоритмдерін білдіреді. Сараптама жүйесінің барлық ережелері "егер <...> , онда <...>".

Теріс пайдаланушылықтарды табу жүзеге асырған жағдайда, сараптама жүйелері, абстракция деңгейі жоғары табиғи тілдегі шабуылдардың моделін сипаттайтын, ережелерді қамтиды. Аномалияларды табу жүзеге асырылған жағдайда, талдау пайдаланушылардың белгілі бір уақыт кезеңі ішінде мінез-құлқын сипаттайтын статистикалық деректер бойынша жасалған ережелер жиынтығы негізінде жүргізіледі. Тиісінше, талдау нәтижесі пайдаланушының шабуылының болуы немесе аномальды мінез-құлқы туралы қорытынды болып табылады. Ережелер жиынтығын сипаттау тілі шабуылдар туралы жинақталған білімді модельдеу үшін жоғары деңгейлі құрал болып табылады. Ереже жиынтығы жаңа шабуылдар немесе жаңа пайдаланушы үлгілері пайда болған кезде жаңартылады. Бұл тәсіл оқиғаларды осалдықтарды пайдалану әрекеттері туралы куәліктердің мәніне және пайдаланылатын қосымшалардың Ақпарат қауіпсіздігі саясатына сәйкестігін табысты талдауға мүмкіндік береді. Бұл тәсілдің негізгі кемшіліктері – шабуылдар туралы білім алу қиындығы және талдау процесінің жылдамдығы төмен болуы.

Статистикалық әдістер – аномалияларды анықтауды іске асыру үшін ең кең қолданылатындардың бірі. Жүйенің немесе пайдаланушының мінез-құлқы белгілі бір уақыт кезеңі ішінде дискретизацияланатын және тиісті профильде сақталатын белгілер жиынтығымен сипатталады (сессияны бастау және аяқтау уақыты, ресурстарды пайдалану ұзақтығы, жады саны, процессорлық уақыт және т.б.).

Статистикалық әдістерді қолдану «қызмет көрсетуден бас тарту» типіндегі шабуылдарды анықтауға мүмкіндік береді, бұл шабуылдар TCP/IP стекіне кіретін коммуникациялық хаттамалардың осалдығын пайдаланады. Мысалы, SYN-flood-шабуыл, шабуылдаушы сұраныс көздерінің жалған өзгеретін IP адрестері бар қосылыстарды орнатуға көптеген сұраныстарды жібергенде, шабуылдау жүйесімен қосылысты орнату процесінің басталғанын растайтын хабар жіберіледі. Қосылыстарды орнату процестері аяқталмайды, бұл жүйелік ресурстардың тапшылығына әкеледі. Шабуылдаушы мінез-құлқы ресми түрде өзара іс-қимыл хаттамасына сәйкес болғандықтан, мұндай шабуылдарды белгілі бір уақыт кезеңінде қосылыстарды орнатуға жіберілген сұраныс саны бойынша ғана анықтауға болады. Ашық қосылыстардың рұқсат етілген санымен бірге қосылысты орнатуға сұрау саны шабуылдардың осы түрін анықтау үшін шекті мәнді анықтайды.

Статистикалық профилі бірнеше түрдегі көрсеткіштерден тұруы мүмкін:

- жұмыстың қарқындылық көрсеткіштері;
- аудит журналдарында тіркелетін оқиғаларды бөлу заңдарын сипаттайтын көрсеткіштер;
- категориялаушы көрсеткіштер (мысалы, жүйеге кірудің салыстырмалы жиілігі);
- сандық көрсеткіштер (мысалы, пайдаланушы қолданатын процессорлық уақыттың немесе енгізу-шығару операцияларының жалпы саны).

Әрбір пайдаланушының ағымдағы мінез-құлқы ағымдағы профильде сипатталады. Аномальды мінез-құлық пайдаланушының ағымдағы профилін оның сақталатын профилімен салыстыру арқылы анықталады.

Уақытша сипаттамаларды қамтымайтын статистикалық көрсеткіштерден тұратын қалыпты мінез-құлық бейіндері былайша құрылады:

- пайдаланушының мінез-құлқының нормалылығы көрсеткіштің әрбір жаңа мәні параметрдің алдыңғы мәндерінің негізінде таңдап алынған кейбір ауқымға сәйкес келуі тиіс дегенді білдіреді. Мұндай тәсілдің негізгі кемшілігі көрсеткіштер мәндерінің априорлық дәлелді байланысының шабуыл жасау әрекеттерімен мүмкін еместігі болып табылады.;
- пайдаланушының мінез-құлқының нормалылығы көрсеткіштің әрбір жаңа мәні бақыланатын параметрдің орташа мәні және оның орташа квадраттық ауытқуы негізінде есептелген сенімді интервалдың шекарасына жатқызылуы тиіс дегенді білдіреді. Осы тәсілдің негізгі артықшылығы-көрсеткіштердің мәнін шабуыл жасау әрекеттерімен априорлы байланыстыру қажеттілігінің болмауы; кемшілік-жұмыс істеудің өзара байланысты

көрсеткіштерін бағалау мүмкін еместігінен тұратын шабуылдарды анықтау процесінде жүйеліліктің болмауы;

- пайдаланушының мінез-құлқының нормалылығы көрсеткіштердің корреляциясын және олардың мәндерінің көрсеткіштің орташа мәні және оның орташа квадраттық ауытқуы негізінде есептелген сенімді интервалға кіруін есепке ала отырып бағаланады.

Уақытша сипаттамаларды қамтитын статистикалық көрсеткіштерден тұратын қалыпты мінез-құлық бейіндері былайша құрылады:

- мінез-құлықтың нормалылығы Марков процестерінің моделі негізінде есептелген басқа жағдайға өту ықтималдығымен анықталады. Әдетте, жүйелік шақырулардың тізбектерін талдау үшін қолданылады;

- мінез-құлықтың нормалылығы көрсеткіштердің мәндерімен және олардың арасындағы уақытша аралықтармен анықталады. Бұл тәсілдің артықшылығы – оқиғалар арасындағы уақыт аралығын есепке алу.

Профильдерді жаңарту пайдаланушылардың мінез-құлқы эволюциясы пайда болған кезде жүргізіледі.

Пайдаланушылардың қалыпты мінез-құлқын сипаттау үшін статистикалық үлгілерді қолдану технологиясы – міндеттерді орындау үшін рұқсат етілген жиынтықтарды қалыптастыруға – негізделген. Ақпарат қауіпсіздігі саясатына сәйкес, рұқсат етілген тапсырмалар тізбесі пайдаланушылардың күтілетін іс-әрекеттерінің үлгілері ретінде ұсынылады (мысалы, белгілі бір файлдарға қол жеткізу) және білім базасында сақталады. Көрсетілген әрекеттер бақыланатын және жүйеде тіркелетін оқиғалармен салыстырылады. Пайдаланушының ағымдағы және шаблонды іс-әрекеттерінде айырмашылықтар анықталған жағдайда, шабуылды анықтау фактісі тіркеледі. Сигналатуралық талдаудан айырмашылығы, бұл әдісте шабуылдардың шаблондары (сигналдары) емес, рұқсат етілген әрекеттердің шаблондары қолданылады.

Нейрондық желілер негізінде анықтау әдістерінің мынандай артықшылықтары бар:

- нейрондық желілер нейрожелілік көріністің жоғары деңгейіне кепілдік бере отырып, осы деректердің толық емес, бұрмаланған және сызықсыз болған жағдайларында да әртүрлі көздерден (источник) түсетін кіріс деректеріне талдау жүргізуге мүмкіндік береді;

- нейрондық желінің парадигмасын дұрыс таңдаған кезде, есептеу жылдамдығы нақты уақыт режимінде жұмыс істеуге қолайлы болуы мүмкін;

- есептеулер көлемі нейрондық желінің парадигмасымен және ондағы элементтердің санымен анықталады, және нейрондық желі идентификациялауға үйренген объектілер санына байланысты емес, яғни нейрондық желі анықтай алатын және идентификациялай алатын шабуылдар санының артуы, шабуылдарды тану уақытының ұлғаюына әкеліп соқпайды.

Нейрондық желілер негізіндегі модельдердің негізгі кемшілігі ретінде, оқыту үшін бастапқы деректердің көлемінің үлкен болуымен байланысты желіні бастапқы оқыту процесінің күрделілігін айту қажет. Сонымен қатар,

нейрондық желілер негізіндегі модельдер басқа да кемшіліктерге ие. Ол нейрондық желі парадигмасымен және оны нақты есепті шешу үшін қолдану ерекшелігімен байланысты.

Шабуылдарды анықтау үшін нейрондық желілер негізіндегі модельдерді міндетті түрде қолдану керек. Қазіргі уақытта шабуылдарды анықтау жүйесінде мұндай модельдердің практикалық қолданылуы бойынша бірқатар эксперименттер жасалған. Көптеген жағдайларда, желілік трафикті талдау кезінде, теріс пайдаланушылықты анықтау үшін, көп қабатты персептрон негізінде нейрожелілік үлгілерді қолдану мәселелері зерттелді. Тәжірибе нәтижелері шабуылдарды анықтаудың тиімді жүйесін әзірлеу үшін бірқатар техникалық қиындықтар бар екенін көрсетті. Олар жүйенің бастапқы деректерді тікелей желілік трафиктен алу қабілетіне және нейрондық желіде талдау үшін бастапқы деректерді ұсынуға байланысты, бірақ нейрондық желінің өзі дәлдік дәрежесі жоғары шабуылдарды тануға мүмкіндік береді.

Нейрондық желі негізінде шабуылдарды анықтау жүйесін әзірлеу кезінде, ең тиімді нейрожелілік архитектураны таңдау міндетті болып табылады. Нейрондық желілердің көптеген архитектуралары бар (көп қабатты персептрондар, өздігінен ұйымдастырылған карталар, қарсы тарату желілері, Хопфилд желілері, екі бағытты ассоциативті жады және т.б.), олар шабуылдарды анықтау жүйелерін модельдеу және синтездеу үшін қолданылуы мүмкін Нейрондық желінің қандай да бір парадигмасын таңдау, бірінші кезекте, басып кіруді анықтау жүйесінде іске асырылатын шабуылдарды анықтауға (теріс пайдаланулардың табу немесе аномалияларды табу) негізделеді. Бұл ретте, шабуылдарды анықтау жүйесінің шабуылдардың жаңа түрлерін тануды үйрену қабілеті болуы өте маңызды, яғни нейрондық желіні қосымша оқыту кезінде нейрондар арасындағы байланыс салмағын өзгертпеу керек, сондықтан желіні толық қайта оқыту қажет.

Шабуылдарды анықтаудың аралас әдістері теріс пайдалануды анықтау және аномалияларды анықтау әдістерінің комбинациясы болып табылады, бұл шабуылдарды анықтаудың барлық тәсілдерінің артықшылықтарын барынша толық пайдалануға мүмкіндік береді. Аралас әдістер негізінде іске асырылған, шабуылдарды анықтау жүйелері білім базасында жинақталған ақпарат негізінде белгілі үлгідегі шабуылдарды тез және дәл анықтай алады; белгілі шабуылдарға қарсы іс-қимыл жөніндегі іс-шаралар кешенін жедел жүзеге асырады; белгісіз шабуылдарды анықтай алады; білім базасында бар шабуылдарға ұқсастық дәрежесін анықтай отырып, өлшемдер негізінде белгісіз шабуылдарға қарсы әрекет етуді жүзеге асыра алады.

### 1.3 IDS түрлері және басып кіруді анықтау жүйелерінің түрлері

IDS мәнін және оның атқаратын функцияларын түсіну қауіпсіздік саясатына қандай IDS түрін қосу керек екенін анықтаудағы негіз болып табылады. Бұл бөлімде IDS-пен байланысты ұғымдар, әрбір типтегі IDS функционалдығы және бір пакетте табудың тәсілдерін іске асыратын гибридті жүйелердің пайда болуы талқыланады.

Кейбір IDS жүйелері білімге негізделген және кең таралған шабуылдардың деректер базасын пайдалана отырып, әкімшілерді басып кіру туралы алдын ала ескертеді. Мінез-құлыққа негізделген IDS жүйелері, керісінше, ресурстарды пайдалануды қадағалай отырып, зиянкестер белсенділігінің белгісі болып табылатын ауытқуларды анықтайды. Кейбір IDS-тер фондық режимде жұмыс істейтін және барлық күдікті пакеттерді сырттан тіркей отырып, белсенділікті пассивті талдайтын жеке қызметтер болып табылады. Басып кіруді анықтаудың басқа да қуатты құралдары стандартты жүйелік құралдардың үйлесімі, өзгертілген конфигурациялар, администратор интуициясымен және тәжірибесімен журналды егжей-тегжейлі жүргізу нәтижесінде алынады.

Қауіпсіздік саласында ең кең тараған IDS типтері жергілікті және желілік IDS жүйелері болып табылады. Жергілікті IDS опциясы неғұрлым кең көлемді болып табылады, өйткені шабуылды анықтау жүйесі әрбір жеке компьютерге орнатылады. Торап өзінің желілік ортасына қарамастан қорғалған болып қалады. Желілік IDS пакеттерді бір құрылғыдан жинап, берілген тораптарға жібермес бұрын оларды талдайды. Желілік IDS әдетте мүмкіндігі шектелген деп еспетеледі, өйткені мобильдік ортада тораптар саны көп болған жағдайда пакеттерді сенімді түрде сүзгіден өткізу және желіні қорғау мүмкін емес.

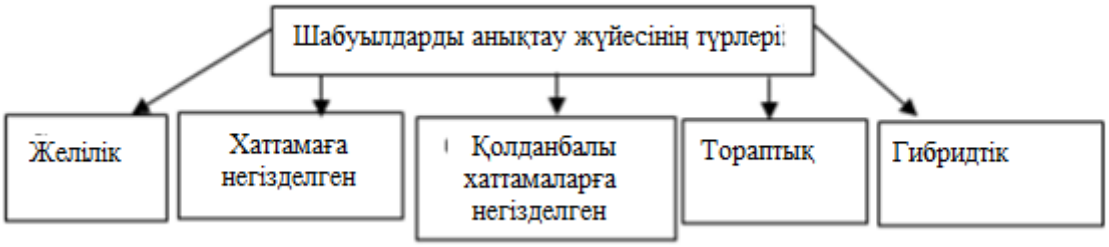
Басып кіруді анықтау жүйелері әдетте екі негізгі санатқа бөлінеді.

Басып кіруді анықтаудың желілік жүйелері (NIDS, ағылш. Network intrusion detection system) – желілік трафикті желінің негізгі тораптарында орналасқан сенсор деректері бойынша талдайды.

Хост деңгейінде басып кіруді анықтау жүйесі (hid S, ағылш. Host-based intrusion detection system) - жүйелік сұраныстарды, қосымшалардың белсенділік логияларын, файлдық жүйенің өзгерістерін және хост деңгейінде болатын басқа да процестерді талдайтын арнайы қызмет арқылы басып кіруді анықтайды [3].

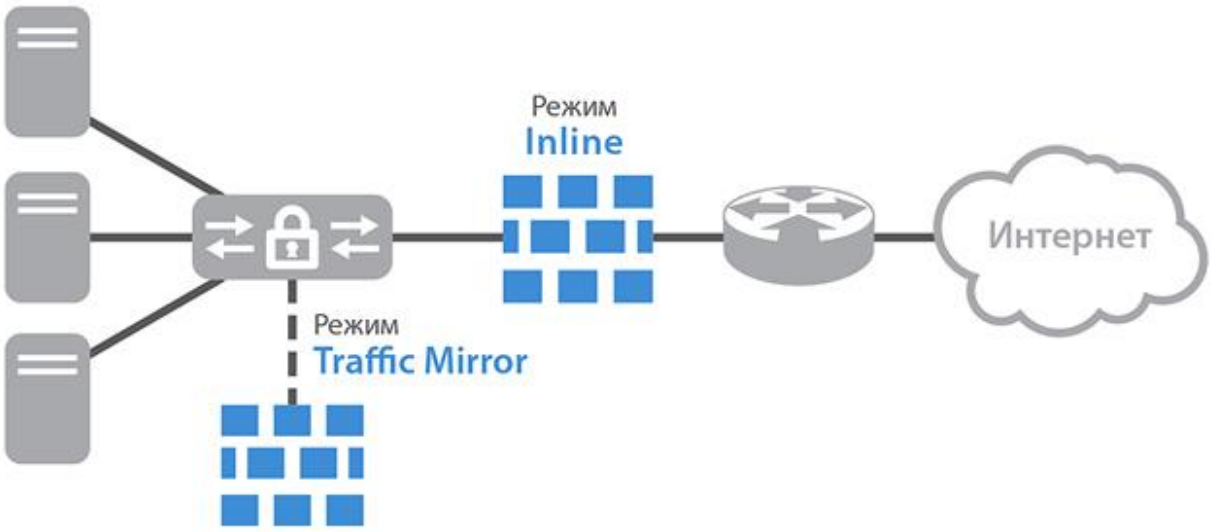
Сонымен қатар, талдау алгоритмдері бойынша басып кіруді анықтау жүйелерінің жіктелуі де бар, ол сигналдардың деректер базасында негізделуі немесе қалыпты («дені сау») режимде жүйенің жұмысын бақылау нәтижелері бойынша эвристикалық тәсілді пайдалануы мүмкін.

Шын мәнінде, басып кіруді анықтау жүйелері пассивті қорғаныс құралы болып табылады. Ақпараттық қауіпсіздік инциденттері тіркеледі және ДК пайдаланушысына немесе желі администраторына есеп түрінде беріледі. Орын алған оқиғалар туралы логтар IDS-қосымшаның арнайы бөліміне және әкімшінің басқару панеліне жазылады. Деректер қауіпсіздігіне төнетін қауіп-қатерлер туралы сигналдардың мұндай жүйелерде одан әрі өңделе алмайды. Деректерді тікелей қорғау және ақпараттық қауіпсіздікті бұзумен күрес үшін, басып кіруді болдырмау жүйесі сияқты белсенді қорғаныс құралдары пайдаланылады.




Сурет 1.1 – Рұқсатсыз басып кіруді (шабуылды) анықтау жүйесінің түрлері

Шабуылды анықтаудың желілік жүйесі (Network-based IDS, NIDS) желілік трафикті тексере отырып, рұқсатсыз кіруді қадағалайды және бірнеше хост арқылы бақылау жүргізеді (Сурет 1.2). Басып кіруді анықтаудың желілік жүйесі хабқа немесе свитчке қосыла отырып, желілік трафикке қол жеткізе алады. Шабуылдарды анықтаудың желілік жүйесінің мысалы Snort болып табылады.




Сурет 1.2 – Шабуылдарды анықтаудың желілік жүйесі

Хаттамада негізделген басып кіруді анықтау жүйесі (Protocol-based IDS, PIDS) бір-бірімен байланысты жүйелермен немесе пайдаланушылар арқылы коммуникациялық хаттамаларды қадағалайтын және талдайтын жүйе (не агент) болып табылады (Сурет 1.1). Веб-сервер үшін мұндай басып кіруді анықтау жүйесі әдетте HTTP және HTTPS хаттамаларын бақылайды. HTTPS хаттамасын пайдаланғанда, басып кіруді анықтау жүйесі HTTPS пакеттерін шифрлағанға және желіге жібергенге дейін көре алатындай белгілі бір интерфейсте орналасуы тиіс.

Қолданбалы хаттамаларға негізделген басып кіруді анықтау жүйесі (Application Protocol-based IDS, ADS) – бұл белгілі бір қосымшалар үшін арнайы хаттамаларды пайдалана отырып, берілетін деректерді бақылау мен

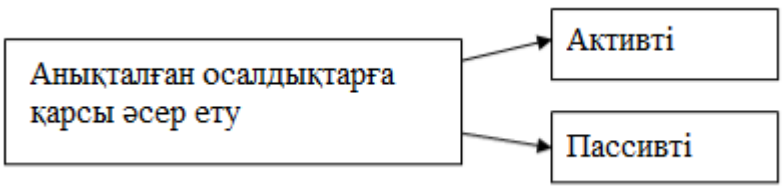
талдауды жүргізетін жүйе (немесе агент). Мысалы, SQL деректер қоры бар веб-серверде басып кіруді анықтау жүйесі серверге берілетін SQL командалардың мазмұнын қадағалайды.

Басып кіруді анықтаудың тораптық жүйесі (Host-based IDS, HIDS) — хосттарда орналасқан жүйе (немесе агент), жүйелік шақыруларды, қосымшалар логтарын, файлдардың модификацияларын (орындалатын, пароль файлдарын, жүйелік деректер базасын), хост жағдайын және басқа да көздерді талдауды пайдалана отырып, басып кіруді қадағалайтын жүйе (немесе агент). Бұл жүйеге мысал ретінде OSSEC-ті алуға болады.

Басып кіруді анықтаудың гибридті жүйесі басып кіруді анықтаудың екі және одан да көп тәсілдерін біріктіреді. Сонымен қатар, желі қауіпсіздігі туралы толық түсінік беру үшін, хосттердегі агенттерден алынған мәліметтер желілік ақпаратпен біріктіріледі. Басып кіруді анықтаудың гибридті жүйесіне мысал ретінде Prelude келтіруге болады. Гетерогенды желіде әр түрлі операциялық желілері бар пайдаланушылар болуының ықтамалдылығы жоғары. Осыған орай, желілік IDS-тің елеулі кемшілігі, әр түрлі TCP/IP-стектерді жүзеге асыру ерекшеліктерін ескеретін, шабуылдарға потенциалды осалдылығы болып табылады.

Рұқсатсыз басып кіруді анықтаудың желілік жүйесі желіаралық экран арқылы өтетін ішкі жергілікті есептеу желісіне шабуылдардан қорғай алады. Желіаралық экрандар дұрыс конфигурацияланбауы мүмкін, яғни қауіпті болуы мүмкін кейбір қосымшалардың қажетсіз трафигін желіге өткізіп жібереді. Порттар желіаралық экраннан пошта немесе басқа жалпы серверге арналған трафигі бар ішкі серверлерге жиі жіберіледі. Рұқсатсыз басып кіруді анықтаудың желілік жүйесі бұл трафикті бақылай алады және ықтимал қауіпті пакеттер туралы сигнал береді. Дұрыс конфигурацияланған басып кіруді анықтаудың желілік жүйесі желіаралық экранның ережелерін қайта тексеріп, қосымшалар серверлері үшін қосымша қорғаныс беруі мүмкін.

Кіруді анықтаудың желілік жүйелері сыртқы шабуылдардан қорғау кезінде пайдалы, алайда олардың басты артықшылықтарының бірі ішкі шабуылдарды және пайдаланушылардың күдікті белсенділігін анықтау қабілеті болып табылады.




Сурет 1.3 – IDS жүйесінің анықталған қауіптерге қарсы әрекет ету тәсілдері.

Жоғарыда аталғандарға қарағанда, белсенді IDS басып кіруге қарсы тұруға тырысады. Олардың іс-әрекеттері ағымдағы қауіпті қосылыстың

үзілуін, сондай-ақ желіаралық экранның конфигурациясын өзгерту жолымен немесе өзге тәсілмен шабуылдаушы толық бұғаттауды қамтуы мүмкін.

Пассивті жүйелер (сурет 1.3) басып кіруді идентификациялаған жағдайда, әдетте желілік шабуыл логын қамтитын болған жағдайлар туралы егжей-тегжейлі есеп жасайды, мысалы, электрондық пошта арқылы қауіпсіздік қызметін хабардар етеді және анықталған осалдықты жою бойынша ұсынымдар береді.

IDS жүзеге асыру тәсілі бойынша бағдарламалық және аппараттық болып бөлінеді. Қазіргі уақытта үй және корпоративтік пайдаланушыларға арналған бағдарламалық қорғау құралдарын өндірушілердің көпшілігі кіруді анықтаудың кіріктірілген жүйесімен үйлескен антивирус, антиспам, проактивті модуль және желіаралық экран сияқты компоненттер енгізілген интеграцияланған шешімдерді ұсынады.

Басып кіруді анықтаудың желілік жүйелерінің подкласстары:

- мөлдір желі IDS (Transparent Network IDS — TNIDS) желілік қосылу үзіліміне орнатылады.

- сенсорлы желілік IDS (Sensor Network IDS — TNIDS) желі сегментіне бір портпен қосылады және осы портқа түсетін трафикті тыңдайды. Егер жергілікті желі коммутацияланатын болса, онда сенсорлы IDS қосылуы трафикті тыңдау үшін қажетті жіберілетін коммутаторлардың айналы порттарына жүргізіледі.

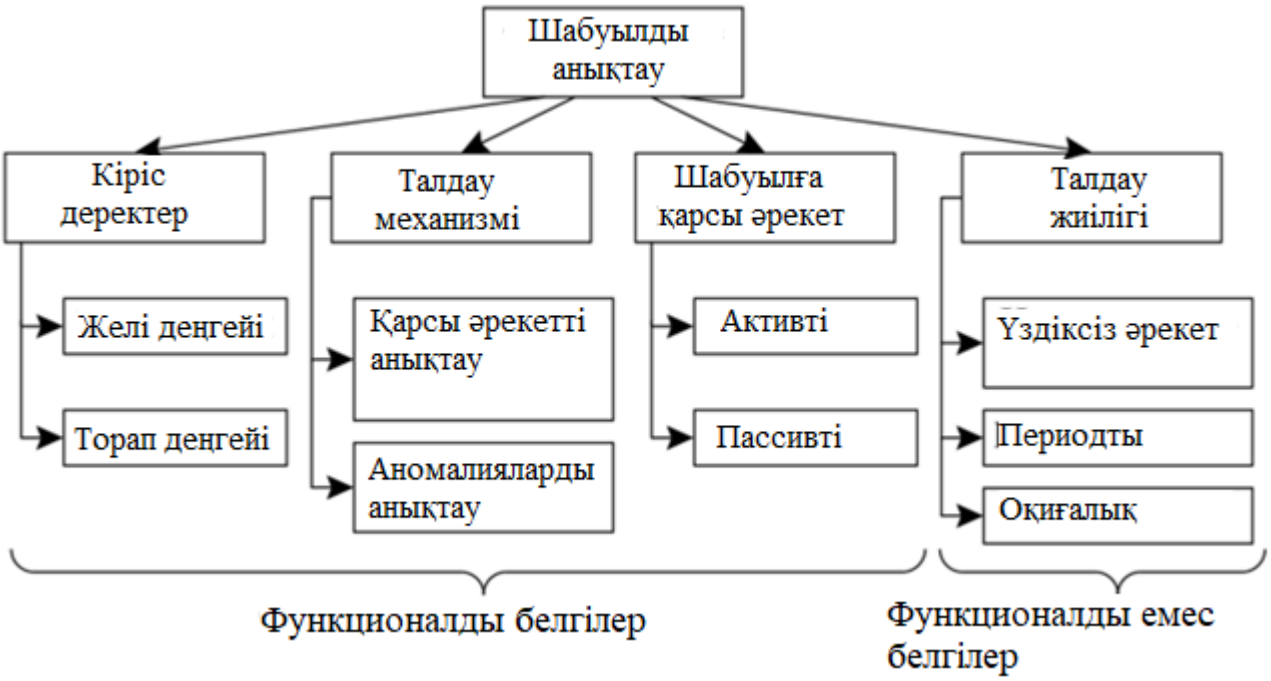
Басып кіруді анықтау жүйесі – пайдаланушыны рұқсатсыз шабуылдардан қорғаудың тиімді құралы, алайда, егер біз толыққанды қауіпсіздік туралы айтатын болсақ, IDS – тек осы жүйенің элементі ғана екенін ұмытпаған жөн. Толық қауіпсіздік-бұл:

- интернет қауіпсіздігі саясаты;
- хостарды қорғау жүйесі;
- желілік аудит;
- маршрутизаторлар базасында қорғау;
- желіаралық экран;
- басып кіруді анықтау жүйесі;
- анықталған шабуылдарға қарсы әрекет ету саясаты.

Тек жоғарыда аталған барлық қорғаныс түрлерін сауатты үйлестіре отырып, пайдаланушы маңызды деректерді сақтау және беру қауіпсіздігі үшін алаңдамауына болады.

### 1.4 Шабуылдарды анықтау жүйелерінің жіктелуі

1.4-суретте функционалды және функционалды емес белгілер негізінде басып кіруді анықтау жүйелерінің жіктелуі ұсынылған. Функционалдық белгілері анықтау процесінің ішкі механизмдерін іске асыру ерекшеліктеріне сәйкес келеді (пайдаланылатын кіріс деректері, талдау тетігі, басып кіруге реакция процесінде АЖ сервистерімен өзара іс-қимылды ұйымдастыру). Функционалды емес белгілер – бұл талдау және анықтау оқиғаларының жиілігіне тәуелділік.




Сурет 1.4 – Рұқсатсыз басып кіруді (шабуылды) анықтау классификациясы.

Деректер көздерінің орналасу негізінде басып кіруді анықтау жүйелерін жіктеу басым болып табылады және шабуылдарды табу үшін пайдаланылатын кіріс ақпаратының түріне негізделеді. Бастапқы ақпаратты жинау үшін деректер көздерінің екі базалық түрі бар: желі деңгейінің датчиктері және торап деңгейінің датчиктері [4].

Желі деңгейінің датчиктері, әдетте, операциялық жүйелердің аудит журналдарын, қосымшалар журналдарын, жүйелік ресурстардың жай-күйі туралы ақпаратты деректер көзі ретінде қолданады. Мысалы, жүйелік файлдардың бүтіндігін бақылау сомалары немесе тізілімнің жүйелік кілттері параметрлерінің мәндері бойынша кезеңдік тексеру сияқты, шабуылды анықтауға мүмкіндік беретін кез келген түйіннің мәліметтері торап жағдайы туралы деректер көзі болуы мүмкін. Анықталған өзгерістер негізінде шабуыл түрін анықтайды. Шабуылға басып кіруді анықтау жүйелерінің дер кезінде реакциясы, бұл жағдайда бақылау кезеңінің шамасымен анықталады. Осылайша, жүйелік белсенділіктің ерекше оқиғаларын (пайдаланушылардың кіруі мен шығуы, жаңа бағдарламалық қамтамасыз етуді орнату, жүйелік ресурстарды пайдалану, әкімшінің қызметі және т.б.) бақылай отырып, желі деңгейінде анықталуы мүмкін емес шабуылдарды анықтауға мүмкіндік береді, мысалы, бақыланатын автоматизацияланған жұмыс орны клавиатурасының шабуылдары.

Желі деңгейінің датчиктері, уақыт режимінде бүкіл трафикті нақты адамға жақын талдай отырып, деректер көзі ретінде тыңдау режимінде желілік адаптерлермен алынатын желілік пакеттер немесе фреймдерді қолданады. Сонымен қатар, маршрутизаторлардың желіаралық экранынан, коммутаторлардан және басып кіруді анықтау жүйелерінің арнайы агенттерінен алынатын оқиғалар туралы ақпарат пайдаланылады. Желі

деңгейінің датчиктері нақты уақыт режиміндегі басып кіруді анықтау жүйесін анықтауды және оған әсер етуді қамтамасыз етеді, оны жүргізу сәтінде шабуыл туралы ақпарат береді.

Архитектураның елеулі айырмашылықтарына және ОЖ жүйелік механизмдерін іске асыруға байланысты ақпарат көздерінің нақты тізбесі нақтылауды талап етеді. Сондықтан бастапқы ақпаратты жинау процесін талдау ОЖ-ның әр түрлі топтары үшін бөлек жүргізген жөн.

Үздіксіз әрекет ететін басып кіруді анықтау жүйесінде датчиктер арнайы деректерді, жағдайды немесе белсенділік түрлерін іздеуде деректер көздерінен ақпаратты үнемі жинайды және өңдейді және олардың пайда болуына қарай күдікті оқиғаларды анықтайды. Мұндай талдау нақты уақыт режимінде жүргізіледі, бірақ деректер көзі мен табу тәсілінің ерекшеліктеріне байланысты оқиғаның пайда болу уақыты мен оқиғаның табылған уақыты арасындағы уақыт аралығы болуы мүмкін. Сонымен қатар, кейбір жағдайларда шабуыл ол анықталғанға дейін аяқталуы мүмкін. Шабуыл мен оны табу арасындағы бұл уақытша кідірістер басып кіруді және қорғалатын объектілерді анықтау жүйелерінің тұрақтылығына байланысты қауіп төндіруі немесе төндірмеуі мүмкін.

Дерек көздерінен алынған ақпаратты талдауға кезеңдік тәсілді іске асыратын басып кіруді анықтау жүйесінде деректер белгіленген уақыт кезеңінде өңделеді. Мысалы, аудиттің жүйелік журналдарына жазулар үздіксіз жүргізіледі, бірақ олар жүйенің ең аз ақпараттық жүктемесі кезінде (түнгі уақытта) талдануы мүмкін. Немесе журналдар мұрағатталады және содан кейін бөлінген АЖО өңделеді. Үздіксіз талдау жүргізу мүмкін болмаған жағдайда ақпаратты қорғауды қамтамасыз ету үшін талдауға мерзімдік тәсілдің кіруін анықтау жүйесінде пайдаланған жөн.

Оқиғалық талдаудың басып кіруін анықтау жүйесінде қолдану әдетте белгілі бір жағдайды жан-жақты терең талдау үшін қолданылады, Мысалы, кең таралған шабуыл анықталған жағдайда. Бұл жағдайда шабуылдарды және оның ықтимал салдарын егжей-тегжейлі талдау үшін қосымша ресурстарды бөлу орынды.

Шабуылдарды анықтау үшін деректерді талдауға екі жалпы тәсіл бар: теріс пайдалануды анықтау және аномалияларды анықтау. Теріс пайдаланушылықты анықтау белгілі үлгідегі шабуылдар туралы жинақталған білім негізінде басып кіруді анықтауды болжайды. Аномалияны анықтау жүйенің қалыпты жай-күйінен ауытқуларды анықтауға негізделеді. Кіруді анықтау жүйесінде пайдаланылатын тәсілге қарамастан, талдау процесі шабуыл белгілері немесе жүйенің қалыпты мінез-құлқының белгілі бір ережелері мен сипаттамалары туралы білім базасының болуын болжайды. Талдау процесінде қандай да бір оқиғаны жүйеде шабуыл жасау әрекеті ретінде түсіндіру мүмкіндігі бағаланады.

Қауіпті пайдаланушылықты анықтау процесі жүйеде нақты сипатталған оқиғалар тізбектерінің пайда болуын бақылау арқылы жүргізіледі. Осы тәсілді

іске асыру үшін математикалық әдістердің кең спектрі қолданылады, мысалы, сигналдық әдіс, сараптамалық жүйелер және күйлерді талдау әдістері.

Аномалияларды анықтау жүйе параметрлерінің мәндерінің ауытқуын және шабуылдар болмаған жағдайда қалыптасқан жүйенің қалыпты жүріс профилінде сақталатын мәндер мен тізбектерден оқиғалар реттілігін анықтау жолымен жүргізіледі. Көрсетілген тәсілді іске асыру үшін математикалық статистика әдістері және жасанды интеллект әдістері қолданылады.

Басып кіруге реакция дегеніміз – басып кіруді анықтаған жағдайда, басып кіруді анықтау жүйелерінің жүзеге асырылатын іс-қимыл реттілігі. Шабуылға реакция таңдау бойынша шешім қабылдау процесі сыртқы әсерден қорғалуы тиіс, әйтпесе қаскүнем ақпараттың қауіпсіздік саясатының бұзылуына басып кіруді анықтау жүйесінің әрекет етуін алдын алуға потенциалды мүмкіндігі бар.

Егер шабуылға реакция жүйенің мінез-құлқын өзгертпейтін, тек әкімшіні басып кіру фактісі туралы хабардар ететін әрекеттер болып табылса, онда реакция пассивті болып саналады. Бұл реакция түрі шабуылдан болатын залалды азайту бойынша ешқандай іс-қимылды көздемейді. Егер шабуылға реакция жүйелік параметрлердің (сессиялардың жабылуы, желілік сервистерді тоқтату және т.б.) мәнін өзгертетін іс-әрекеттерді қамтыса, басып кіруді анықтау жүйесінің реакциясы белсенді деп аталады. Белсенді әрекет ету тетіктері персоналды хабардар етіп қана қоймай, сонымен қатар шабуылдан болатын ықтимал залалды азайтуға бағытталған шаралар кешенін жүргізу бойынша шешім қабылдауға автоматты түрде қолдау көрсетуді қамтамасыз етеді. Іс-шаралар спектрі желіаралық экрандарды конфигурациялаудан бастап және контратакалау құралдарын қолданумен аяқталатын болуы мүмкін.

### 1.5 Басып кіруді анықтау жүйелерінің архитектурасы

Қорғалатын АЖ ерекшелігіне байланысты, басып кіруді анықтау жүйесін құру үшін әртүрлі тәсілдер пайдаланылуы мүмкін. Сонымен қатар, бұл жағдайда бір жүйеге кіруді анықтаудың бір жүйесін қолдану жақсы шешім болуы мүмкін. Алайда, ресурстарға қол жеткізудің анық белгіленген кестелері бар желілік және қолданбалы сервистерінің көп саны бар күрделі аумақтық бөлінген желілік инфрақұрылым жағдайында шабуылдарды анықтау жөніндегі талаптарды орындау үшін басып кіруді анықтаудың бір жүйесін қолдану жеткіліксіз болуы мүмкін. Бұл талаптарды қанағаттандыру үшін кіруді анықтаудың бірнеше жүйесі қажет болуы мүмкін, олардың әрқайсысы АЖ-нің белгілі бір кіші жүйесіне немесе компонентіне сәйкес келетін болады. Бұл ретте басып кіруді анықтаудың бірнеше жүйелерімен жиналған деректердің корреляциясын және олардың жалпыланған талдауын жүргізу қажет.

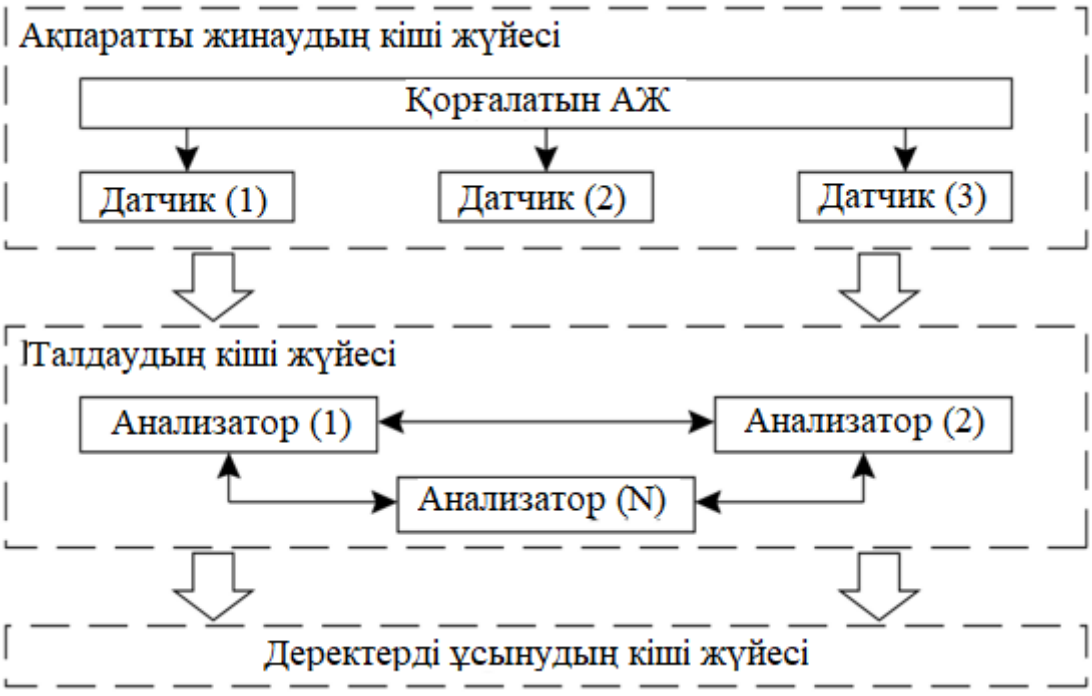
Шабуылдарды табу жүйелерін құру архитектурасын таңдаудың мақсаты пәрменді және тиімді түрде шабуылдарды табу функцияларын іске асыру болып табылады, ол үшін архитектураға көзқарасты таңдайды (басып кіруді анықтаудың бір немесе бірнеше жүйелерін қолдану) және деректерді талдау

функцияларын орталықтандырудың қажетті дәрежесін анықтайды. Көп деңгейлі инфрақұрылымы бар басып кіруді анықтау жүйелерін жобалау талап етілетін функцияларды іске асыруға мүмкіндік беретін архитектураның бірнеше нұсқаларының болуын болжайды.

Орталықтандырылған архитектура көптеген датчиктер жинауды және бастапқы өңдеуді, талдау мен іздеу корреляция сияқты деректерді бірден-бір компонентте жүзеге асырады  Мұндай тәсілдің артықшылығы – қарапайым жобалау. Алайда, архитектураның мұндай нұсқасын таңдаудың салдары шағын АЖ қорғау үшін ғана ауқымдылықтың төмендігі мен практикалық қолданылуы болып табылады.

Масштабталуын жақсартуға қызмет ету процесінде неғұрлым жоғары деңгейге берілетін деректер көлемін қысқарту мақсатында орталықсыздандырылған компоненттердегі бастапқы деректерді өңдеудің кейбір функцияларын іске асыру арқылы қол жеткізуге болады. Компоненттер жиынтығы талдауды жүзеге асырады және деректерді қорытынды өңдеу үшін тек қажетті ақпаратты ғана орталық консольге бере отырып, деректердің корреляция дәрежесін белгілейді. Мұндай архитектурасы бар жүйе үшін бұғаттау және конфигурациялау үдерісі қиындайды, өйткені табылған шабуылдар туралы хабарламалар орталық консольге жетуі қажет [5].

Жалпы жағдайда басып кіруді анықтау жүйелері ақпаратты жинау, деректерді талдау және ұсыну сияқты кіші жүйелерден тұрады. Басып кіруді аныцқтау жүйесінің жалпы құрылымы 1.5-суретте көрсетілген.




Сурет 1.5 – Басып кіруді анықтау жүйесінің жалпы құрылымы.

Ақпаратты жинаудың кіші жүйесі қорғалатын нейрондық желінің жұмысы туралы деректерді жинақтайды. Ақпаратты жинау үшін саны

нейрондық желінің ерекшелігіне байланысты автономды модуль – датчиктер қолданылады. Жиналған ақпараттың сипаты бойынша датчиктердің келесі түрлерін бөледі:

- қосымшалар датчиктері қорғалатын жүйенің бағдарламалық қамтамасыз ету жұмысы туралы деректерді жинауды жүзеге асырады;
- хост датчиктері қорғалатын жүйенің жұмыс станциясының жұмыс істеуі туралы деректерді жинауды жүзеге асырады;
- желі датчиктері желілік трафикті бағалау үшін деректерді жинауды жүзеге асырады;
- желіаралық датчиктер желілер арасында айналатын деректер сипаттамаларын жинайды.

Басып кіруді анықтау жүйесі датчиктердің келтірілген үлгілерінен кез келген комбинацияны қамтуы мүмкін.

Талдаудың кіші жүйесі талдаудың бір немесе бірнеше модулінен тұрады. Әрбір модуль шабуыл немесе басып кірудің белгілі бір түрін іздеуді орындайды. Талдаушыға арналған кіріс деректері ақпаратты жинаудың кіші жүйесінен немесе басқа талдаушыдан алынған ақпарат болып табылады. Ішкі жүйенің жұмыс нәтижесі – бұл қорғалатын нейрондық желінің жағдайы туралы индикация. Талдағыш санкцияланбаған әрекеттердің табылғандығы туралы хабарлаған жағдайда, шығыс деректерінде басып кірудің немесе шабуылдың болу фактісін растайтын қорытындылар болуы мүмкін [6].

Деректерді ұсынудың кіші жүйесі қорғалатын АЖ жағдайы туралы мүдделі тұлғаларды хабардар ету үшін қажет. Басып кіруді анықтаудың кейбір жүйелерінде қорғалатын АЖ-нің белгілі бір кіші жүйелерін бақылайтын пайдаланушылар тобының болуы болжанады. Сондықтан мұндай басып кіруді анықтау жүйесінде қол жетімділікті шектеу, топтық саясат, өкілеттілік және т.б. қолданылады.

Басып кіруді анықтаудың қазіргі жүйесінің құрылымдарына келесі негізгі кемшіліктер тән:

1) құрастырудың жалпы әдістемесінің болмауы. Ең алдымен, мұны терминологиядағы жалпы келісімдердің жетіспеушілігімен түсіндіруге болады.

2) аппараттық ресурстарды жоғары тұтыну. АЖ-да ауытқуларды анықтауға негізделген қолда бар басып кіруді анықтау жүйелері АЖ-ның әрбір оқиғасы үшін профайлды жаңартуды орындайды, бұл ресурстарды Елеулі тұтынуға және АЖ-ның жалпы өнімділігін азайтуға әкеп соғады. Теріс пайдалануды анықтау принципі бойынша жұмыс істейтін басып кіруді анықтау жүйесі жұмыс кезінде өзінің көптеген ережелерін өңдейтін сараптама жүйелерінің командалық интерпретаторларының көмегімен шабуылдар мен басып Кірулер сигналдарын кодтайды, бұл сондай-ақ ресурстардың қосымша жұмсалуына алып келеді.

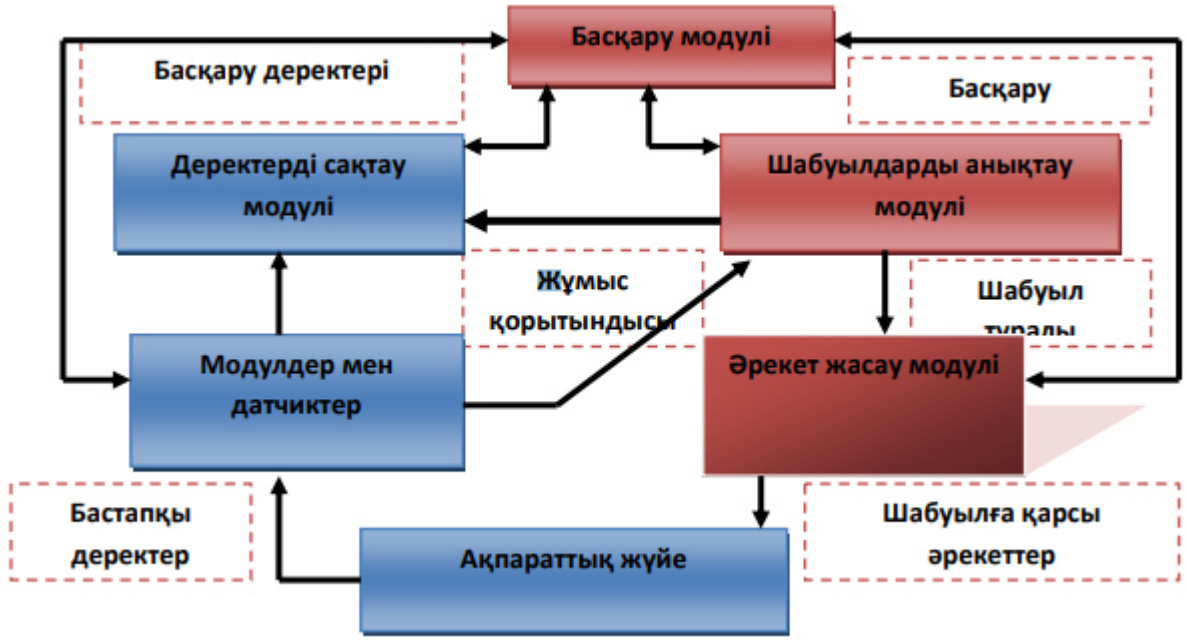
3) жеткіліксіз әмбебаптылық, аппараттық-бағдарламалық платформаларға қатты тәуелділік. Негізгі себеп-басып кіруді анықтаудың

көптеген жүйелері басқа жүйелерге тән емес белгілі бір құрылғылар мен бағдарламалардың орындалуын бақылайды.

4) жаңартудың төмен мүмкіндіктері. Жаңа кіші жүйені басып кіруді анықтаудың жаңартылған жүйесіне енгізу оның құрамдауыштары арасындағы өзара іс-қимылдың әмбебап тетігінің болуын талап етеді. Қазіргі уақытта мұндай тетік әзірленді (көпагенттік тәсіл), бірақ тиісті Даму алған жоқ.

5) қызмет көрсетуші персоналдың біліктілігіне қойылатын жоғары талаптар. Басып кіруді анықтау жүйесін орнату қауіпсіздік саласындағы білімдерден ерекшеленетін қосымша дағдыларды талап етеді. Мысалы, теріс пайдалануды анықтау жүйелерінде көптеген ережелерді жаңарту сараптамалық жүйенің мамандандырылған білімін талап етеді. Бұл аномалияны анықтау жүйесінің статистикалық өлшемдері туралы айтуға болады.

6) нақты жағдайларда басып кіруді анықтау жүйесін қолдану тиімділігін бағалау әдістемесінің болмауы. Шабуылды анықтау жүйесінің типтік сәулеті 1.6-суретте келтірілген.




Сурет 1.6 – Шабуылды анықтау жүйесінің типтік сәулеті.

### 1.6 Шабуылдарды анықтау технологиясы

Желілік және ақпараттық технологиялар тез өзгеретіні сонша, қатынауды шектеуші жүйелер, ЖЭ, аутентификациялау жүйесі сияқты статикалық қорғаныш тетіктері көптеген жағдайларда тиімді қорғауды қамтамасыз ете алмайды. Сондықтан қауіпсіздікті бұзуды жедел анықтауға және болдырмауға мүмкіндік беретін динамикалық әдістер қажет. Қол жеткізуді бақылаудың дәстүрлі үлгілерінің көмегімен сәйкестендірілуі мүмкін емес бұзушылықтарды анықтауға мүмкіндік беретін технологиялардың бірі шабуылдарды анықтау технологиясы болып табылады.

Шын мәнінде, шабуылдарды анықтау процесі корпоративтік желіде орын алатын күдікті әрекеттерді бағалау процесі болып табылады. Былайша айтқанда, шабуылдарды анықтау (intrusion detection) – бұл есептеу немесе желілік ресурстарға бағытталған күдікті қызметке сәйкестендіру және ден қою процесі.

### 1.7 Шабуылдарға әрекет ету тәсілдері

Шабуыл тек қана анықталмауы керек, сонымен қатар оған дұрыс және уақтылы әрекет ету қажет. Қолданыстағы жүйелерде әрекет ету әдістерінің кең спектрі қолданылады, оларды үш санатқа бөлуге болады:

- хабарлама;
- сақтау;
- белсенді әрекет ету.

Қандай да бір реакцияны қолдану көптеген факторларға байланысты.

Хабарлама. Хабарлаудың ең қарапайым және кең таралған әдісі қауіпсіздік әкімшісіне шабуылдарды анықтау жүйесінің консолына шабуыл туралы хабарламаларды жіберу болып табылады. Мұндай консоль ұйымда қауіпсіздік үшін жауап беретін әрбір қызметкерге орнатылмауы мүмкін, бұдан басқа, бұл қызметкерлерді қауіпсіздіктің барлық оқиғалары қызықтыруы мүмкін емес, сондықтан хабарлаудың өзге де тетіктерін қолдану қажет. Бұл тетіктер хабарламаларды электрондық пошта, пейджерге, факс немесе телефон арқылы жіберуі мүмкін [7].

«Хабарлама» санатына сондай-ақ басқару тізбектерін басқа жүйелерге, мысалы желілік басқару жүйелеріне немесе ЖЭ-ға жіберу жатады.

Сақтау. «Сақтау» санатына әрекет етудің екі нұсқасы жатады:

- оқиғаны ДБ-да тіркеу;
- нақты уақыт ауқымында шабуыл жасау.

Бірінші нұсқа басқа қорғау жүйелерінде кең таралған. Екінші нұсқаны іске асыру үшін желіге шабуылдаушы компанияны «өткізіп жіберу» және оның барлық әрекеттерін тіркеу қажет. Бұл қауіпсіздік әкімшісіне содан кейін нақты уақыт ауқымында (немесе берілген жылдамдықпен) шабуылдаушы жүзеге асырған барлық іс-қимылдарды жаңғыртуға, «сәтті» шабуылдарды талдауға және оларды одан әрі болдырмауға, сондай-ақ талқылау процесінде жиналған деректерді пайдалануға мүмкіндік береді.

Белсенді әрекет ету. Бұл санатқа келесі әрекет ету нұсқалары жатады:

- шабуылшының жұмысын бұғаттау;
- шабуыл түйіні бар сессияны аяқтау;
- желілік жабдықтарды және қорғаныс құралдарын басқару.

Бір жағынан, ден қою тетіктерінің бұл санаты жеткілікті тиімді, ал екінші жағынан, ұқыпты пайдалануды талап етеді, өйткені дұрыс қолданбау барлық КАЖ жұмысқа қабілеттілігінің бұзылуына әкелуі мүмкін.

## 2 Практикалық бөлім

Кез келген кәсіпорын сайтында белгілі бір деректер базасы болады және қаскүнем (хакер) иньекциялар немесе шелл арқылы веб-сайттағы деректерге шабуыл жасауы мүмкін. Дипломдық жобада Алматы энергетика және байланыс университетінің сайтына жасалған шабуылдарды анықтау және бұғаттау жүзеге асырылды. Жұмыс кезінде шабуылды немесе рұқсатсыз басып кіруді анықтау үшін Django фреймворкі қолданылды. Django Python программалау тілінде жазылған аса танымал және жартылай функционалды серверлік веб-фреймворк болвп табылады. Осы модульда әзірлеу ортасын орнату және онымен жұмыс жасауды бастау көрсетіледі.

### 2.1 Python бағдарламалау тілі

Python – әзірлеушінің өнімділігін және кодтың оқылуын арттыруға бағытталған жалпы мақсаттағы жоғары деңгейлі бағдарламалау тілі (сурет 2.1). Python ядросының синтаксисі ең аз. Сонымен қатар стандартты кітапхана пайдалы функциялардың үлкен көлемін қамтиды.

Python құрылымдық, объектілі-бағытталған, функционалдық, императивті және аспектілі-бағытталған бағдарламалауды қолдайды. Негізгі архитектуралық ерекшеліктер – динамикалық типизация, жадыны автоматты басқару, толық интроспекция, ерекшеліктерді өңдеу механизмі, көп ағынды есептеулерді қолдау, деректердің жоғары деңгейлі құрылымы. Өз кезегінде, пакеттерге бірігуі мүмкін модульдерге бағдарламаларды бөлу қолдайды.

Python эталондық іске асырылуы-белсенді қолданылатын платформалардың көпшілігін қолдайтын CPython интерпретаторы. Ол Python Software Foundation License еркін лицензиясымен таралады, оны кез келген қосымшаларда, соның ішінде проприетарлық қолданбаларда шектеусіз пайдалануға мүмкіндік береді. Компиляция мүмкіндігі бар JVM үшін интерпретатор іске асыру бар, CLR, LLVM, басқа да тәуелсіз іске асыру. PyPy жобасы Python-бағдарламаларды орындау жылдамдығын айтарлықтай арттыратын JIT-компиляцияны пайдаланады.


Сурет 2.1 – Python бағдарламалық тілі

Python-белсенді дамып келе жатқан бағдарламалау тілі, тілдік қасиеттерді қосу/өзгерту жаңа нұсқалары шамамен екі жарым жылда бір рет шығады. Тіл ресми стандарттауға ұшырамады, де-факто стандартының рөлін тіл авторының бақылауымен жасалған CPython орындайды.

Python динамикалық типтеуді қолдайды, яғни айнымалы түрі тек орындау кезінде анықталады. Сондықтан «айнымалы мәнін тағайындау «орнына» кейбір атауымен мәнді байланыстыру» туралы айту жақсы. Python-да енгізілген түрлері бар: түйреуіш, жол, Unicode-жол, еркін дәлдіктің бүтін саны, өзгермелі үтірмен сан, кешенді сан және т.б. Python коллекцияларынан енгізілген: тізім, кортеж (өзгермейтін тізім), сөздік, көптеген және басқалар. Барлық мәндер объектілер болып табылады, оның ішінде функциялар, әдістер, модульдер, сыныптар.

Жаңа түрді қосу класты (class) жазу немесе кеңейту модулінде жаңа түрді (мысалы, C тілінде жазылған) анықтау арқылы болады. Кластар жүйесі мұраға (жалғыз және көпше) және метапрограммалауға қолдау көрсетеді. Көптеген кірістірілген түрлер мен кеңейтулердің типтерінен мұрагерлік болуы мүмкін.

Барлық объектілер сілтемелік және атомдық болып бөлінеді. Атомдық int, long complex және басқа да. Атомдық объектілерді беру кезінде олардың мәні көшіріледі, ал сілтемелік үшін тек объектіге көрсеткіш көшіріледі,осылайша, берілгеннен кейін екі айнымалылар бірдей мәнді пайдаланады. Сілтеме нысандары өзгертілетін және өзгермейтін болады. Мысалы, жолдар мен кортеждер өзгермейтін, ал тізімдер, сөздіктер және басқа да көптеген нысандар өзгеретін болады.

### 2.2 Веб-қолданбаларға арналған Django фреймфоркі.

Django – Python тіліндегі веб-қолданбалар үшін арналған фреймворк. Фреймворктің негізгі принциптерінің бірі-DRY (don't repeat yourself). Django Веб-жүйелері бір немесе бірнеше қосымшалардан құрылады, олар иеліктен және жалғанады. Бұл фреймворктың кейбір басқа да сәулет ерекшеліктерінің бірі (мысалы, Ruby on Rails). Сонымен қатар, көптеген басқа фреймворктерге

қарағанда, Django URL түлегіштері айқын конфигурацияланады (тұрақты өрнектердің көмегімен), автоматты түрде контроллерлер құрылымынан орнатылмайды.

Django Apache басқарумен және PostgreSQL деректер қоры ретінде жұмыс істеу үшін жобаланған. Қазіргі уақытта, PostgreSQL-ден басқа, Django басқа ДББЖ-мен жұмыс істей алады: MySQL (MariaDB), SQLite, Microsoft SQL Server, DB2, Firebird, SQL Anywhere және Oracle. Django деректер базасымен жұмыс істеу үшін жеке ORM қолданады, онда Деректер моделі Python кластарымен сипатталады және ол бойынша деректер базасының схемасы жасалады.

Django архитектурасы «модель-көрініс-Контроллер» (MVC) сияқты. MVC классикалық моделінің контроллері Django-да көрініс (View) деп аталатын деңгейге сәйкес келеді, ал ұсыныстың презентациялық логикасы Django-да шаблондардың деңгейімен (Templates) жүзеге асырылады. Осыған байланысты Django деңгейлік архитектурасын жиі «үлгі-үлгі-көрініс» (MTV) деп атайды.

Бастапқыда Django-ның әзірлеуі жаңалық ресурстарымен неғұрлым ыңғайлы жұмысты қамтамасыз ету үшін жүргізілді, бұл архитектураға қатты әсер етті: фреймворк ақпараттық сипаттағы веб-сайттарды жылдам әзірлеуге көмектесетін бірқатар құралдарды ұсынады. Мысалы, әзірлеушіге сайттың әкімшілік бөлігі үшін контроллерлер мен беттер жасауды талап етпейді, Django-да жасалған кез келген сайтқа қосуға болатын мазмұнды басқару үшін кірістірілген бағдарлама бар және ол бір серверде бірнеше сайттарды бірден басқара алады. Әкімшілік қосымша барлық жасалған іс-әрекеттерді хаттамалай отырып, сайттың толтырудың кез келген нысандарын жасауға, өзгертуге және беруге мүмкіндік береді және пайдаланушылар мен топтарды басқару үшін интерфейсті ұсынады (әр объект бойынша құқық белгілеумен).

Django веб-фреймворк Instagram, Disqus, Mozilla, The Washington Times, Pinterest, lamoda және т. б. сияқты ірі және танымал сай-тарда қолданылады.

Кейбір Django мүмкіндіктері:

- ORM, транзакцияларды қолдайтын ДБ қол жеткізу API;
- әкімші интерфейсі, бар көптеген тілдерге аудармалары бар;
- тұрақты өрнектер негізіндегі URL менеджері;
- тег және мұрагерлік үлгілердің кеңейтілген жүйесі;
- кештеу жүйесі;
- интернационалдандыру;
- кез келген Django-сайттарға орнатуға болатын қосылатын бағдарламалар архитектурасы;
- generic views — контроллерлер функцияларының үлгілері;
- авторизация және аутентификация, сыртқы аутентификация модульдерін қосу: LDAP, OpenID және басқалар.
- қосымша сұраныстарды өңдеушілерді құру үшін сүзгілер жүйесі («middleware»), мысалы дистрибутивке кіргендер сияқты кештеу, сығу, URL-ды қалпына келтіру және жасырын сессияларды қолдау үшін сүзгілер жүйесі;

- Формамен жұмыс істеуге арналған кітапхана (мұралау, қолда бар ДБ үлгісі бойынша формалар құру);

- әкімшілік қосымша арқылы қол жетімді үлгі және деректер үлгілері бойынша орнатылған автоматты құжаттама.

Кейбір фреймворк компоненттері өзара әлсіз байланысты, сондықтан оларды тек ұқсас етіп ауыстыруға болады. Бірақ кейбір (мысалы, ORM) бұл өте оңай емес. Фреймворк ядросына енгізілген мүмкіндіктерден басқа, оның мүмкіндіктерін кеңейтетін пакеттер бар.

Django базасында еркін лицензияда таратылатын көптеген дайын шешімдер әзірленді, оның ішінде интернет-дүкендерді басқаруға арналған жүйелер, мазмұнды басқарудың әмбебап жүйелері, сондай-ақ тар бағытталған жобалар [8].

Django артықшылықтарына назар аударамыз, ол сапалы код пен Мөлдір жазу үшін қажетті барлық веб әзірлеудің жылдам шешімі ғана емес, сондай-ақ белгілі бір бизнес клиенттерімен, сондай-ақ әзірлеушілермен жұмыс істеу үшін тамаша платформа болып табылады:

1) Жылдамдық. Django әзірлеушілерге бағдарламаны мүмкіндігінше тез жасауға көмектесу үшін әзірленген. Бұл Django осы кезеңдердің әрқайсысында уақыт пен ресурстарды үнемдейтін идеяны қалыптастыру, жобаны әзірлеу және шығару кіреді. Осылайша, оны дедлайн мәселесі басымдыққа ие әзірлеушілер үшін тамаша шешім деп атауға болады.

2) Толық жинақтау. Django он қосымша функциялармен жұмыс істейді, олар пайдаланушы аутентификациясымен, сайт карталарымен, мазмұнды әкімшілендірумен, RSS және т.б. елеулі көмектеседі. Бұл аспектілер веб-әзірлеудің әрбір кезеңін жүзеге асыруға көмектеседі.

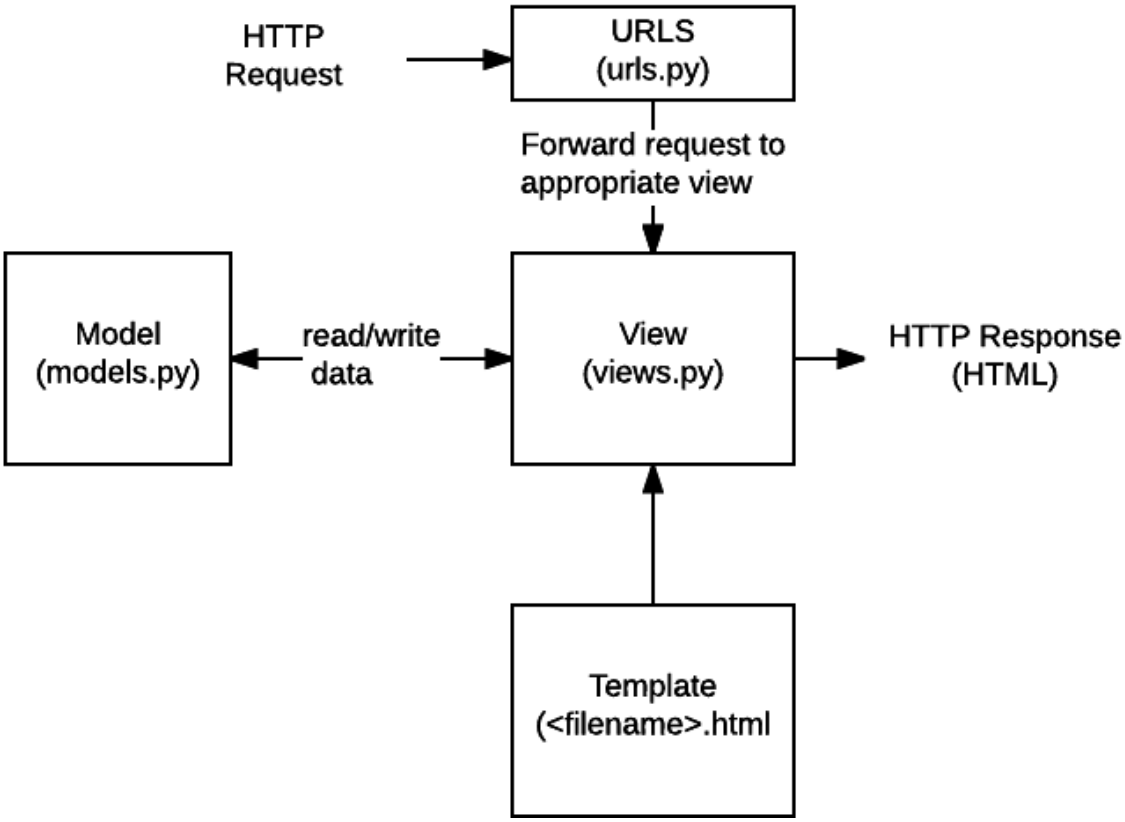
3) Қауіпсіздік. Django-да жұмыс істей отырып, сіз қауіпсіздікпен байланысты және қауіп-қатер жоба. Логин мен парольдерді тиімді пайдалану үшін пайдаланушы аутентификация жүйесі кілт болып табылады.

4) Масштабтау. фреймворк Django ең жоғары трафиктермен жұмыс істеу үшін ең қолайлы. Демек, жүктелген сайттар көп Django-ны трафикке байланысты талаптарды қанағаттандыру үшін пайдаланады.

5) Жан–жақтылық. контент менеджменті, ғылыми есептеу платформалары, тіпті ірі ұйымдар-осының барлығын Django көмегімен тиімді орындауға болады.

Дәстүрлі ақпараттық веб-сайтта, веб-бағдарлама веб-браузерден HTTP сұрауларын күтеді (немесе басқа клиент). Сұрау алынған кезде, бағдарлама URL-мекенжайының негізінде не қажет екенін әзірлейді (мүмкін POST немесе GET сұрау ақпараттары). Талап етілуіне байланысты, ол ақпаратты деректер базасынан оқи немесе жаза алады немесе сұрау салуды қанағаттандыру үшін қажетті басқа да міндеттерді орындай алады. Қосымша веб-браузерге жауапты қайтарады, браузерді көрсету үшін жиі динамикалық HTML бетін жасап, алынған деректерді HTML үлгісіне кірістіреді.

Django-да жазылған веб-бағдарламалар, әдетте, осы қадамдардың әрқайсысы өңделетін кодты жеке файлдарға топтайды, ол 2.2-суретте көрсетілген.




Сурет 2.2 – Django-да жазылған веб-бағдарламалардың жеке файлдық топтары

1) URLs. Бір функцияның көмегімен әрбір URL мекенжайынан сұрауларды өңдеуге болады, дегенмен, әр ресурсты өңдеу үшін жеке функцияны жазу әлдеқайда ыңғайлы. URL-mapper http сұрауларын сұрау URL негізінде тиісті көрініске қайта бағыттау үшін пайдаланылады. URL-mapper сондай-ақ берілген үлгіге сәйкес URL мекен-жайынан деректерді шығарып, оларды дәлел ретінде тиісті функцияға жібере алады.

2) View. Көрініс (view) - HTTP сұрауларын алатын және жауаптарды қайтаратын сұрауларды өңдеуші функциясы • View модель арқылы деректерге қол жеткізуге болады (сұраныстарды қанағаттандыру және шаблондарға жауап беру үшін қажет).

3) Models. Модельдер қолданба деректер құрылымын анықтайтын және деректер базасына сұрау салуларды басқару (қосу, өзгерту, жою) және орындау үшін тетіктерді ұсынатын Python нысандары болып табылады;

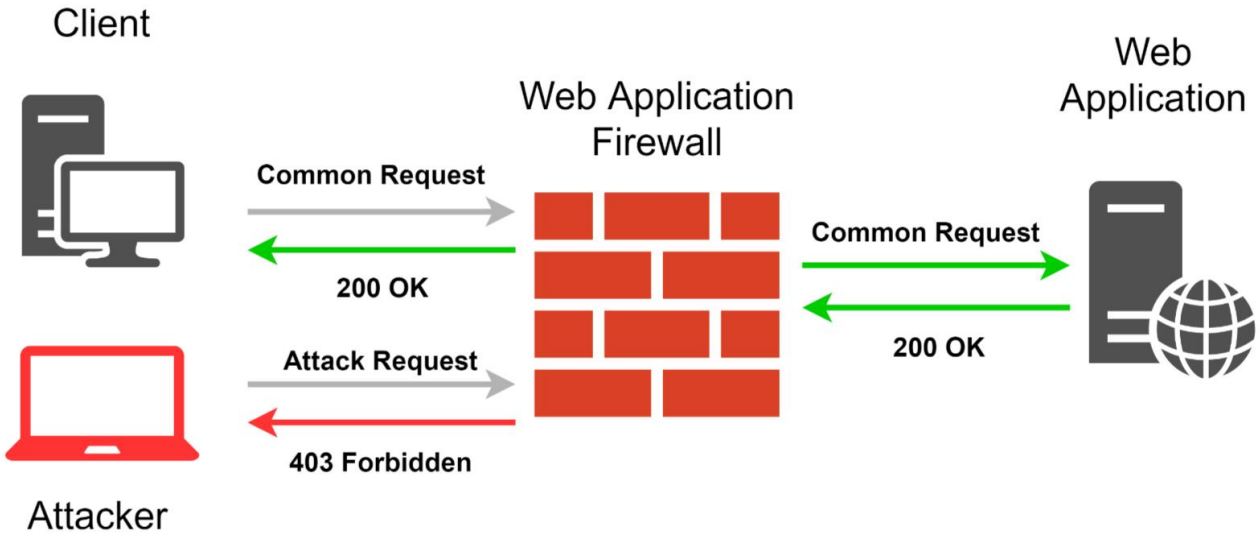
4) Templates. Template (үлгі) - бұл маңызды мазмұнды көрсету үшін пайдаланылатын қою өрістері бар беттің құрылымын немесе белгілеуін анықтайтын мәтіндік файл. View HTML беттерін HTML үлгілерін пайдаланып және оларды модельден (model) деректермен толтыра алады. Үлгі HTML

міндетті емес, кез келген файлдардың құрылымын анықтау үшін пайдаланылуы мүмкін.

Django веб-қосымшалары модельдер деп аталатын Python нысандары арқылы деректерді өңдейді және сұрайды. Модельдер сақталатын деректердің құрылымын, соның ішінде өрістер түрлерін және, мүмкін, олардың ең үлкен өлшемін, әдепкі мәндерін, таңдау тізімінің параметрлерін, құжаттама анықтамасының мәтінін, пішіндер белгілерінің мәтінін және т.б. анықтайды. Сіз пайдаланғыңыз келетін деректер базасын таңдағаннан кейін, сізге тікелей оған жүгінудің қажеті жоқ - сіз жай ғана модель құрылымы мен басқа код жазылады, ал Django деректер базасына жүгіну бойынша барлық қажетсіз жұмысты өңдейді.

### 2.3 Bypass waf шабуылдары

Соңғы уақытта WAF (сурет 2.3) өте танымал болды, вендорлар әртүрлі баға санаттарында, жеткізу жиынтықтары мен түрлі тұтынушыларға арналған нұсқаларда — шағын бизнестен ірі корпорацияларға дейін көптеген шешімдер ұсынады. Қазіргі заманғы WAF танымал, өйткені веб-қосымшаларды қорғаудың кешенді құралы болып саналады және қамтылған міндеттердің кең спектрі бар, сондықтан веб-қосымшаларды әзірлеушілер кейбір қауіпсіздік мәселелерінде оған сене алады, бірақ бұл шешім абсолютті қорғауға кепілдік бере алмайды.




Сурет 2.3 – Web application firewall

Оның негізгі функциясы-WAF талдауына сәйкес, кейбір ауытқулар бар немесе шабуылдаушы вектор байқалады. Мұндай талдау заңды пайдаланушылардың веб-қосымшамен өзара іс-қимылын қиындатпауы тиіс, сонымен бірге шабуылдардың кез келген әрекеттерін дәл және уақтылы анықтау керек. Мұндай функционалдылықты іске асыру үшін WAF әзірлеушілері әдетте тұрақты сөздерді, токенайзерлерді, мінез-құлық талдауын, бедел талдауын, сондай-ақ машиналық оқытуды қолданады, және

көбінесе осы технологиялардың барлығы бірлесіп қолданылады. Сонымен қатар, WAF басқа функционалдылықты да ұсына алады: DDoS-тен қорғау, шабуылдаушылардың IP-адрестерін бұғаттау, күдікті IP-адрестерді қадағалау, security-тақырыптарды қосу (X-XSS-Protection, X-Frame-Options, etc...), cookie-ге http-only жалауын қосу, HSTS механизмін енгізу, CSRF-таңбалардың функционалдығын қосу. Сондай-ақ, кейбір WAF-да JavaScript-та жазылған клиент модулі бар.

Әрине, WAF хакерлер мен пентестерлердің жұмысы үшін бірқатар қиындықтар жасайды. Осалдықтарды анықтау және пайдалану, егер, әрине, шабуылдаушы нақты WAF айналып өту тәсілдері 0day-тиімді 0day белгілі болмаса, көп еңбекті қажет ететін міндет болып табылады. WAF қорғау астында веб-қосымшаларды талдау кезінде автоматтандырылған сканерлерді қолдану пайдасыз. WAF сайттарды кем дегенде scriptkiddies-тен сенімді қорғайды. Дегенмен, тәжірибелі маман немесе хакер тиісті уәждемесі жоқ, сондай-ақ қарап шығу жолдарын іздеу үшін көп уақыт жұмсауға емес, шеше алады. Жеке айта кету керек, күрделі және көпфункционалды веб-қолданба неғұрлым көп болса, соғұрлым ықтимал әсер ету аймағы көп және соғұрлым WAF айналып өту жолын табу оңай болады.

### 2.4 Бағдарламалық құрылымдағы шелл – код

Шеллкод(ағылш. shellcode, қабықшаны іске қосу коды) – бұл екілік орындалатын код, әдетте командалық процессорға басқаруды береді, мысалы '/bin/sh' Unix shell, 'command.com 'MS-DOS және' cmd ішінде. Microsoft Windows операциялық жүйелерінде exe'. Шелл-код командалық қабықшаға қол жеткізуді қамтамасыз ететін эксплойттың пайдалы жүктемесі ретінде пайдаланылуы мүмкін (ағылш. shell) компьютерлік жүйеде.

Қашықтағы осалдықты пайдалану кезінде шелл-код осал компьютердің TCP алдын ала берілген портын аша алады, ол арқылы командалық қабыққа одан әрі қатынауды жүзеге асырады, мұндай код портқа байланыстырушы деп аталады (ағылш. port binding shellcode). Егер шелл-код брандмауэрді немесе NAT айналып өту мақсатында жасалатын шабуылдаушы компьютердің портына қосылуды жүзеге асырса, онда мұндай код кері қаптама деп аталады.

Шелл-код әдетте пайдаланылатын бағдарламаның жадына енгізіледі, содан кейін оған стекті асыра толтыру жолымен немесе буфераны көп мөлшерде толтырған кезде немесе форматты жолдың шабуылдарын пайдалана отырып басқару беріледі. Шелл-кодты басқару енгізілген шеллкодтың мекен-жайымен стекте қайтару мекен-жайын қайта жазумен, шақырылатын функциялардың мекен-жайларын қайта жазумен немесе үзу өңдегіштерін өзгертумен жүзеге асырылады. Бұл нәтиже-бұзу үшін командалық жолды ашатын шелл-кодты орындау.

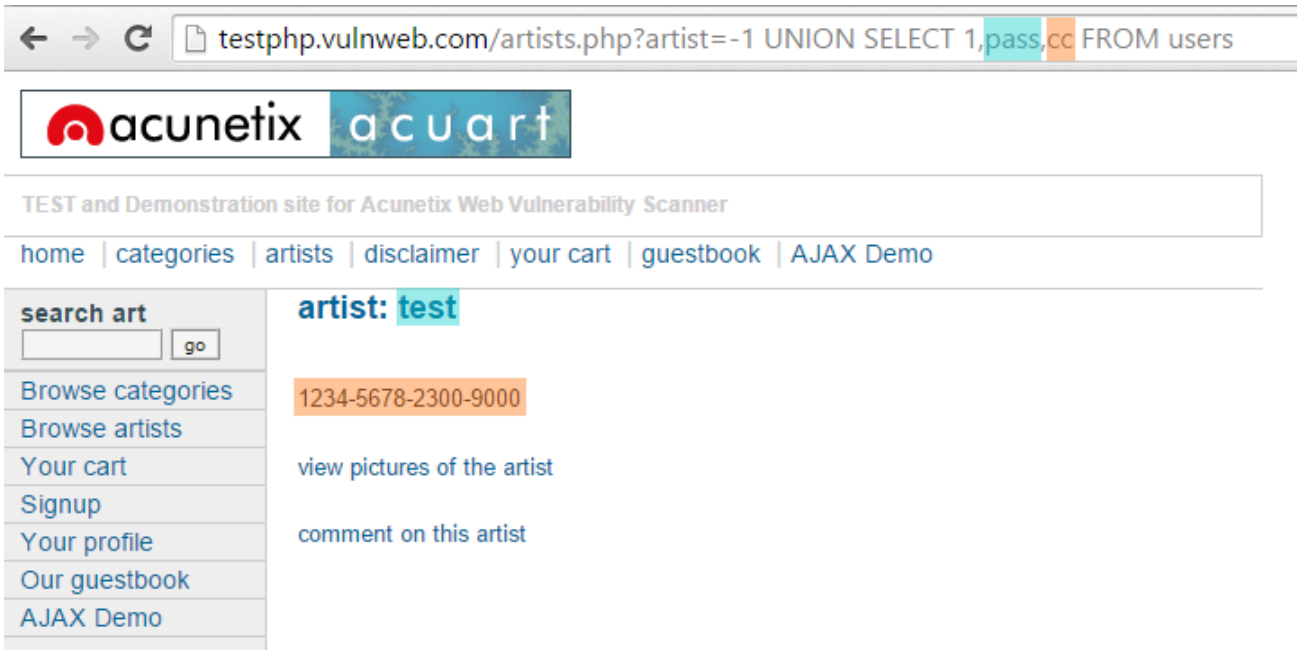
Бұзушылар шабуыл жасыратын әдістерді жиі пайдалана отырып, шелл кодтарын жазады. Олар жиі басып кіруді анықтау жүйелері кез келген кіріс шабуылды қалай танитынын анықтауға тырысады. Әдетте, шелл-кодқа тән құрылымдарды іздеуде барлық кіріс пакеттерді қарайды (көбінесе қоқыс

кодтарының үлкен массиві, қарапайым жағдайда NOP-тер); егер ол осындай құрылымды тапса, пакет өзінің мақсатына жеткенше жойылады. Бұл жағдайда СОВ әлсіз позициясы шын мәнінде жақсы іздеуді жүзеге асырмауы, әйтпесе ол тым көп уақыт алады және осылайша интернетпен байланысты баяулатады.

Шелл коды әрдайым қабық аты бар жолды қамтиды. Мұндай жолдан тұратын барлық кіріс пакеттер әрқашан көз алдында күдікті ретінде қарастырылады. Сондай-ақ, кейбір қосымшалар галфавиттік емес-сандық енгізуді қабылдамайды (олар A-z, A-Z, 0-9 теру шеңберінен және бірнеше басқа символдардан шығатын символдарды қабылдамайды.)

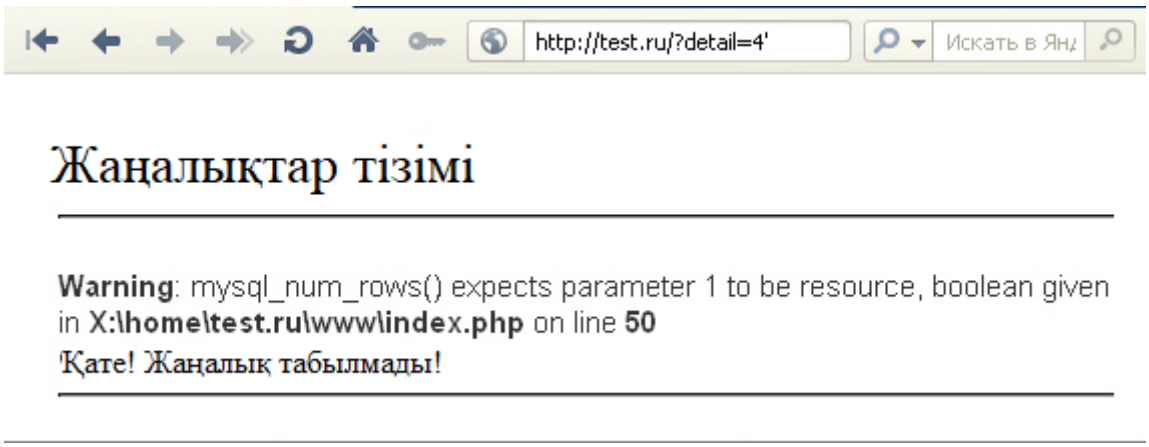
### 2.5 Кәсіпорын сайтына жасалған шабуылдар және оларды анықтау жүйесінің модулі

SQL инъекция – бұл SQL динамикалық операторларын іске қосатын шабуыл, нұсқаудың белгілі бір бөлігін түсіндіре отырып немесе әрқашан шынайы болатын шартты қоса отырып. Ол веб-қосымшалар архитектурасындағы тесіктерге бағытталған және SQL операторлары зиянды SQL-кодты орындау үшін пайдаланады. 2.4-суретте веб-парақшаға жасалған SQL инъекция келтірілген.




Сурет 2.4 – Веб-парақшаға жасалған SQL инъекция

Test.ru деп аталатын тесттік сайтта егжей-тегжейлі қарала алатын жаңалықтар тізімі бар, оның мекен-жайы test.ru/?detail=1. Яғни GET сұранысы арқылы detail айнымалысы 1 мәнін (ол жаңалықтар кестесінің идентификаторы болып табылады) береді. Сұранысты ?detail=1' немесе ?detail=1" мәніне өзгертіп, оны серверге жіберген кезде қателік шықса, демек сайт SQL инъекцияларға қарсы тұра алмайды (сурет 2.5).



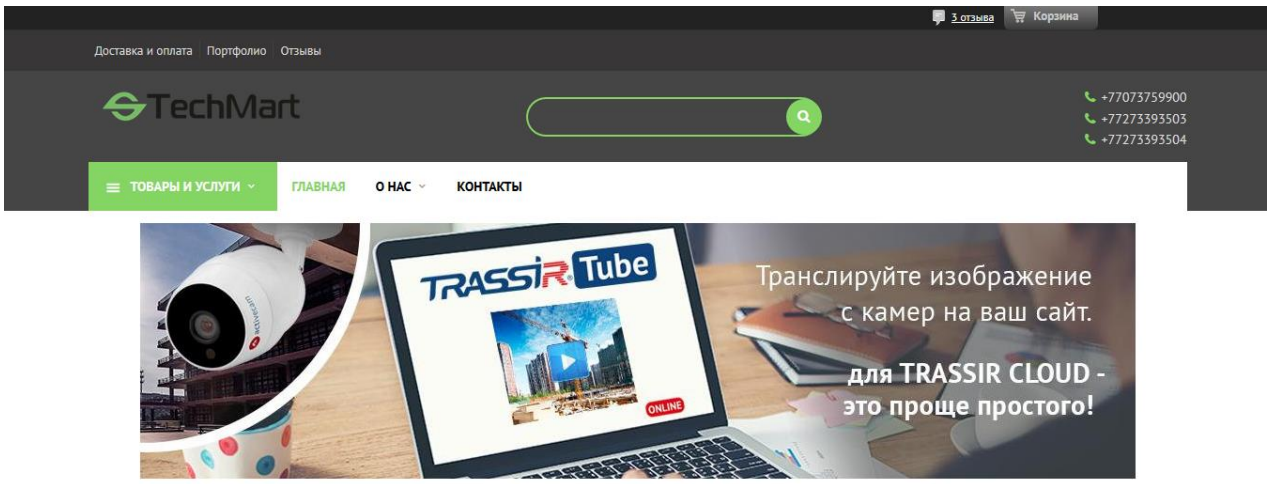

Сурет 2.5 – Осалдыққа тексеру кезінде шыққан қателік

XSS (ағылш. Cross-Site Scripting) – веб-жүйеге берілетін зиянды код бетін (ол осы бетті ашқан кезде пайдаланушының компьютерде Орындалатын болады) енгізуден және осы кодтың қаскүнемнің веб-серверімен өзара әрекеттестігінен тұратын шабуыл түрі. «Кодты енгізу» шабуылының бір түрі болып табылады.

Мұндай шабуылдардың ерекшелігі зиянды код оған кеңейтілген қолжетімділікті алу үшін немесе пайдаланушының авторизациялық деректерін алу үшін веб-жүйеде пайдаланушының авторизациясын пайдалана алады. Зиянды код бетке веб-сервердегі осалдық арқылы да, пайдаланушының компьютеріндегі осалдық арқылы да енгізілуі мүмкін.

Көп уақыт бойы бағдарламашылар оларды қауіпсіз деп санай отырып, оларға тиісті көңіл бөлмеді. Алайда бұл пікір қате: бетте немесе HTTP-Cookie-де өте осал деректер болуы мүмкін (мысалы, әкімші сессиясының идентификаторы немесе төлем құжаттарының нөмірі), ал CSRF-дан қорғау жоқ жерде шабуылдаушы пайдаланушыға қол жетімді кез келген әрекеттерді орындай алады. Желі аралық скриптинг DoS-шабуыл жасау үшін пайдаланылуы мүмкін.

Дипломдық жұмыстың тапсырмасы бойынша, шабуыл жасау үшін қауіпсіздік жүйесі тауарларын сату ісіне арналған «Trassir» компаниясының сайты таңдап алынды (2.6-сурет).

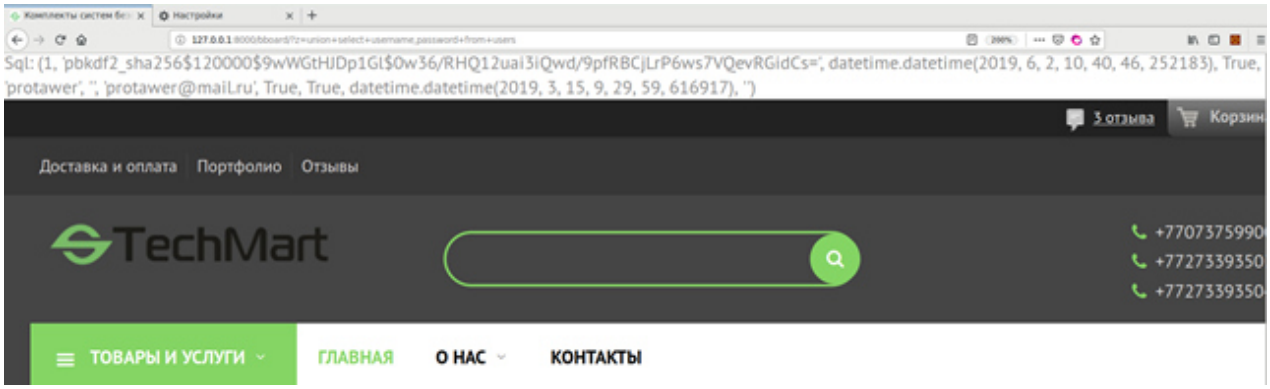



Сурет 2.6 – Кәсіпорынның веб-сайты

DOM-модельде XSS JavaScript сценарийі ішінде деректерді өңдеу кезінде клиент жағында пайда болады. Бұл XSS түрі осындай атау алды, өйткені Dom (Document Object Model) арқылы іске асырылады — бағдарлама мен сценарийлерге HTML және XML-құжаттардың мазмұнына қол жеткізуге, сондай-ақ мұндай құжаттардың мазмұнын, құрылымын және ресімделуін өзгертуге мүмкіндік беретін платформа мен тілге тәуелді емес бағдарламалық интерфейс. Дұрыс сүзілмеген жағдайда Dom шабуылданатын сайтты түрлендіруге және JavaScript-кодты шабуылданатын сайттың контексінде орындауға қол жеткізуге болады. <script>alert(document.cookie);</script> кодын іздеу ортасына теріп, шабуыл жасалады (2.7-сурет).


Сурет 2.7 – Кәсіпорын сайтына жасалға шабуыл

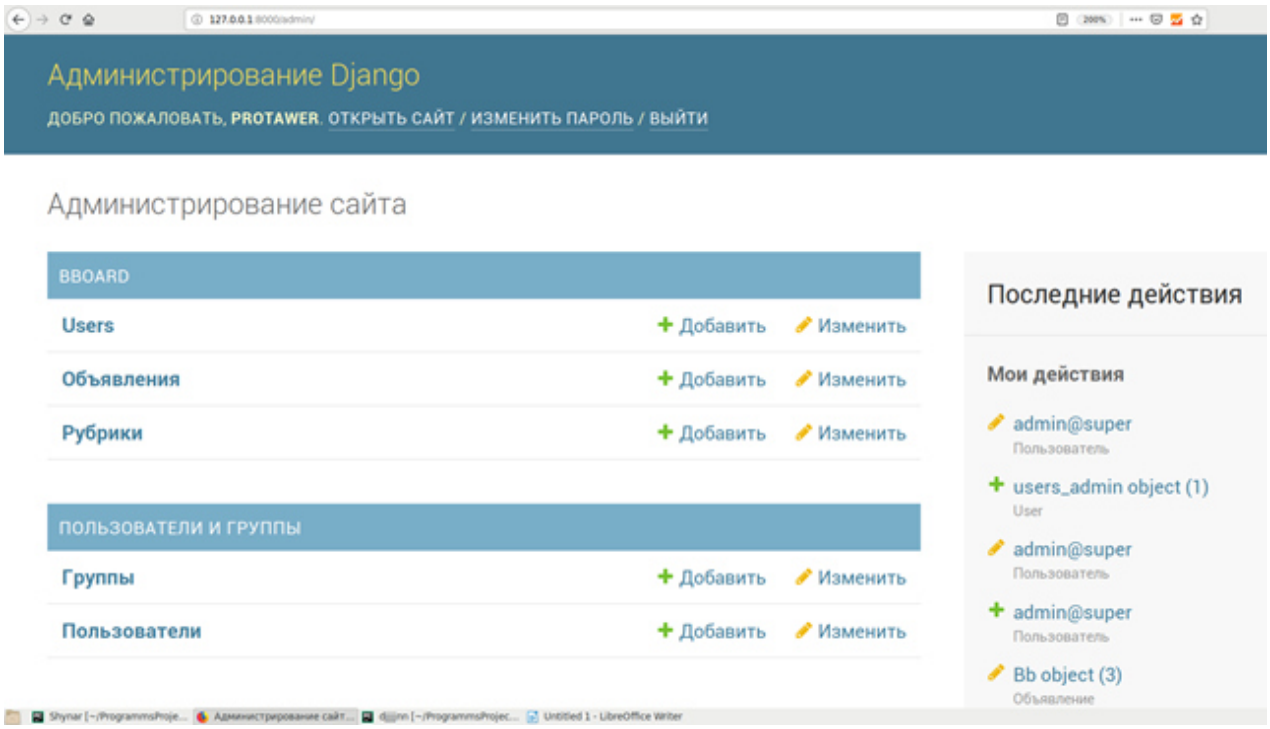
z=union+select+*+from+users кодымен URL параметрі арқылы шабуыл жасалады. 2.8-суретте көрсетілген шабуылда қолданушылардың құпия сөзі шифрланған, шабуылдаушы оны дешифрлау арқылы, пайдаланушы аккаунтына қол жеткізе алады. Сонымен қатар, қолданушы поштасының ашылуы, социалды инженерияға әкеледі, яғни брутфорс шабуыл жасалады.




Сурет 2.8 – Кәсіпорын сайтына жасалған шабуыл

Шабуыл кезінде дешифрланған ақпараттар арқылы администратор атынан кіріп, сайттағы деректер туралы барлық ақпаратты (2.9-сурет) алуға болады:

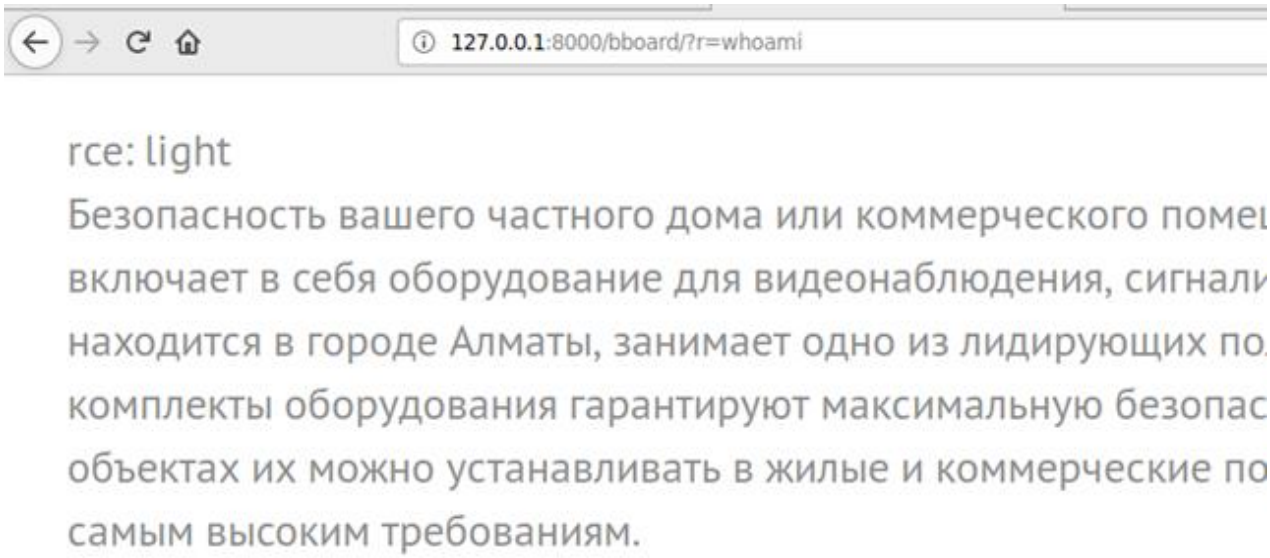
- жаңа қолданушылар, хабарландырулар, топтар және т.б. енгізуге;
- қолданушылардың логин мен құпия сөзін қарауға, оларды жоюға;
- хабарландыруларды жоюға, құрылымын өзгертуге;
- топ құрамындағы қолданушыларды өзгертуге және т.б.




Сурет 2.9 – Сайттағы деректер туралы ақпарат

RCE-ең қауіпті осалдықтардың бірі. 100% жағдайда серверлік скриптке кодты қашықтан енгізу мүмкіндігі бұзылды ресурсқа әкеледі. RCE көмегімен зиянкестер веб-шеллаларды немесе кез келген басқа да зиянды кодты орналастыра отырып, шабуылданатын сайттың серверіне бірден қол жеткізеді.

Біздің тәжірибемізде RCE хакерлік серверлерде орналастырылған скриптерді пайдаланған, олар зиянды құрамдас бөліктердің, Шелл және т.б. вирустардың болуын қадағалаған жағдайлар кездеседі. ?r=whoami параметрімен RCE шабуыл жасауға болады.




Сурет 2.10 – Кәсіпорын сайтын жаслаған шабуыл

Сайтқа жасалған шабуылдарды анықтау үшін Python программалау тілінде алдымен, сайтқа жіберілген сұраныстарды тексеретін белгілі бір ережелер қатары жазылады, ол 2.11-суретте келтірілген.

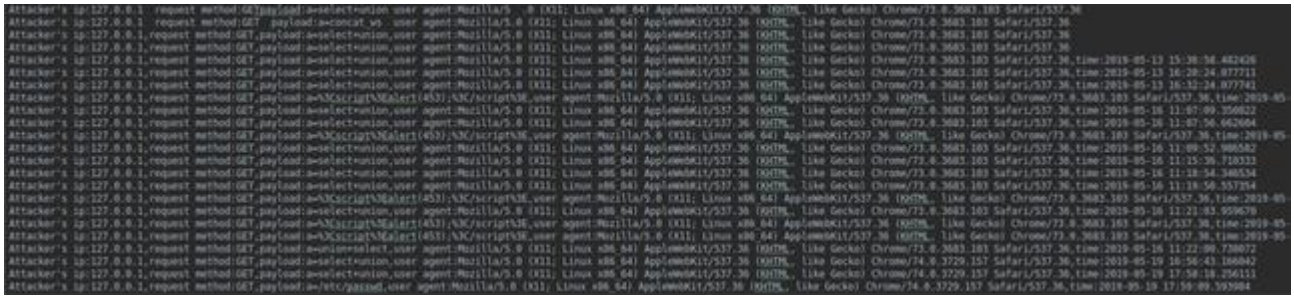
```
rules=['select',
       'etc',
       'passwd',
        'script',
       'order',
       'ls -l',
       'rm -rf',
       '/../../',
       '{{',
       '}}',
       'group+by',
       'concat',
       'php:',
       'base64',
       '@import',
       '%(HOME(DRIVE|PATH)|SYSTEM(DRIVE|ROOT)|WINDIR|USER(DOMAIN|PROFILE|NAME)|((LOCAL)?APP|PROGRAM)DATA)%',
       'bunionb.+?bselectb',
```

Сурет 2.11 – Python-да жазылған ережелер

Рұқстасыз басып кірулерді анықтау мақсатсында келген сұраныстарды сигнатурлы талдау жасайтын алгоритм әзірленді. Сонымен қатар, шабуылдарды анықтау жүйесінің модулі python urldecode көмегімен url encode bypass шабуылдарынан қорғалған (сурет 2.12).

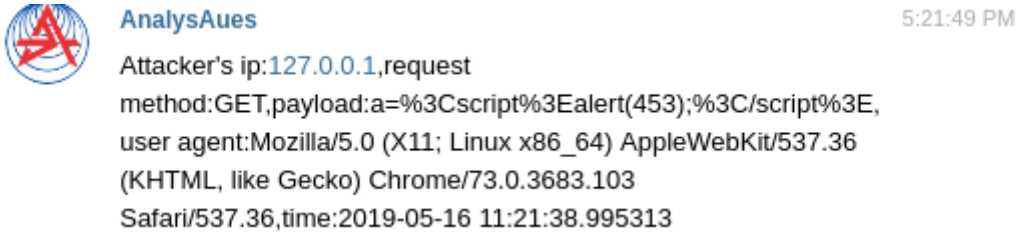

Сурет 2.12 – шабуылдарды анықтау жүйесінің модулі python urldecode

Келген сұранымдарды алдымен дешифрлау және кіші әріппен жазу процесі жүзеге асады, кейін жоғарыда жазылған ережелер бойынша тексеріледі. Егер ережелердің барлығына сәйкес келетін болса, сервер жауп жібереді. Шабуыл жасалғаны белгілі болса, модуль алдағы іс-әрекеттерді тексеру үшін лог файлды генерациялайды. Лог файлда (сурет 2.13) қаскүнемнің (шабуылдаушының) ip-мекен-жайы, оның браузері мен операциялық жүйесі, яғни user-agent, сұраныс тәсілі және сұраныс жіберілген уақыт жазылады.



Сурет 2.13 – log файл құрылымы

Қауіпсіздік деңгейін жоғарылату үшін, сайт иесін немесе администраторды жасалған шабуылдар туралы ескерту қажет. Бұл қызметті рұқстасыз басып кіруді анықтау жүйесі моділінің бөлігі болып табылатын бот атқарады. Бот әрбір 60 секунд сайын лог файлды тексеріп отырады, файлда жаңа өзгерістер табылған кезде, осы жазбаларды сайт иесіне Telegram қосымшасына жіберіп отырады (сурет 2.14).




Сурет 2.14 – Администарторға келген хабарлама

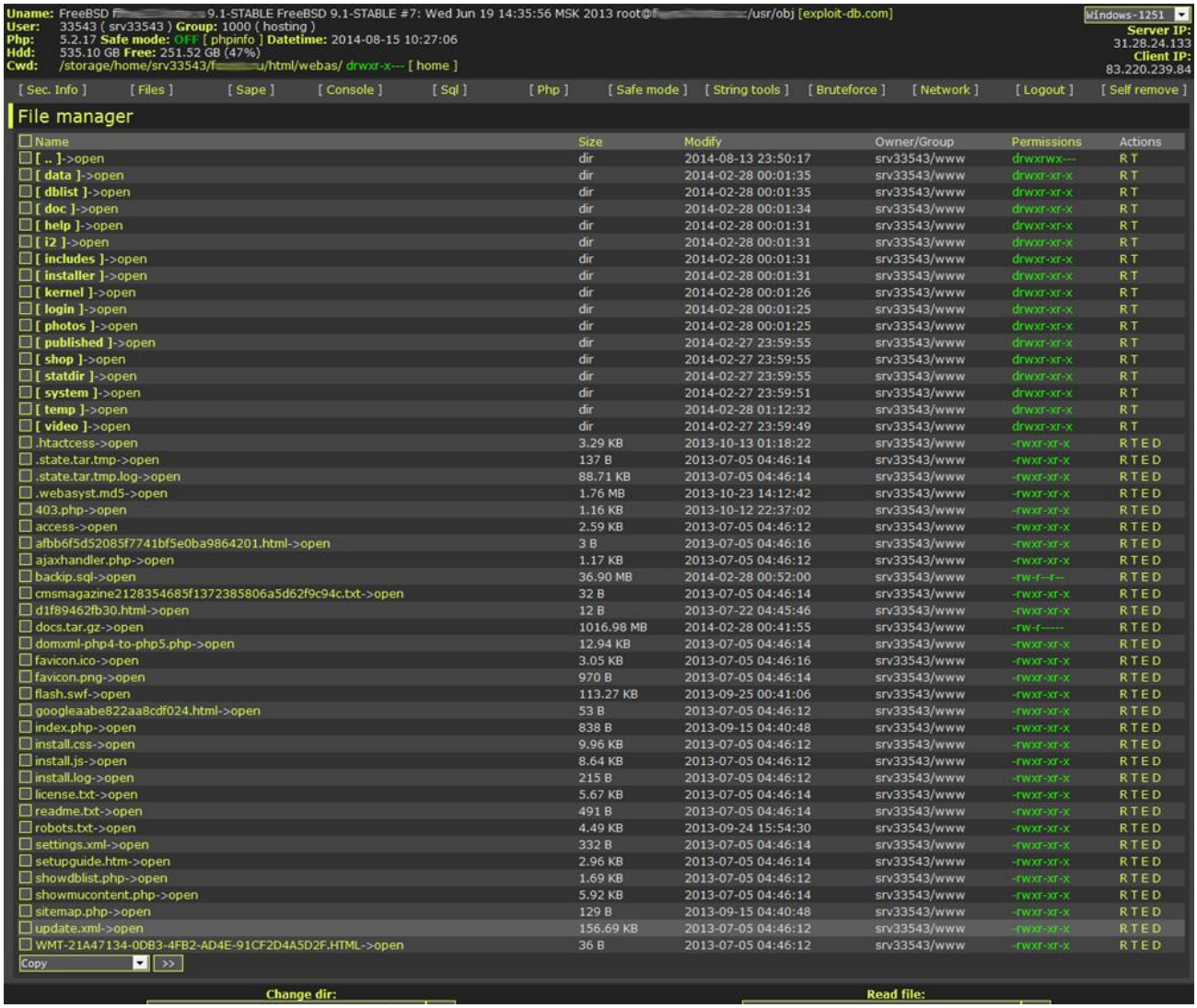
Командалық жолдың интерпретаторы немесе shell (Shell-қабығы) - бұл пайдаланушы командаларын қабылдап, оларды орындайтын бағдарлама.

Қабықшаның (оболочка) функцияларына жатады:

- пайдаланушымен өзара әрекеттесу (командалық жолды редакциялау, командалардың тарихы және т.б.);
- атау үлгілерін өңдеу (кеңейту) («*», «?»және т. б.);
- командаларды енгізу/шығару қайта бағыттау;
- тапсырмаларды басқару.

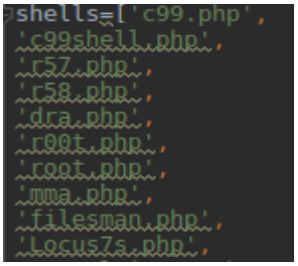
Сонымен қатар, shell-бұл арнайы бағдарламалау тілі (сурет 2.15), онда айнымалы, while, if, for және т.б., функциялар және көп нәрсе бар. Ол күнделікті есептерді автоматтандыру үшін күрделі емес сценарийлерді, сондай-ақ өте күрделі бағдарламаларды жазуға мүмкіндік береді (мысалы, Unix хосттардың көпшілігін іске қосу және тоқтату shell тілінде сценарийлер жасалады).

Әдетте шелл деп хакерлер серверге жүктейтін және оның көмегімен серверді одан әрі басқаруды жүзеге асыратын скрипт білдіреді. Іздеу сұрауымен көптеген шеллдарды табуға болады және олардың танымалдығы сөзсіз өсіп келеді. Жаңа бастаған хакерлер оны бір жерге жүктеуге тырысады.

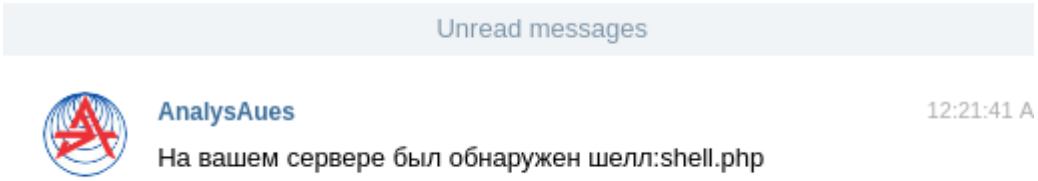



Сурет 2.15 – Хакерлер арасында кеңінен қолданылатын шелл көрінісі

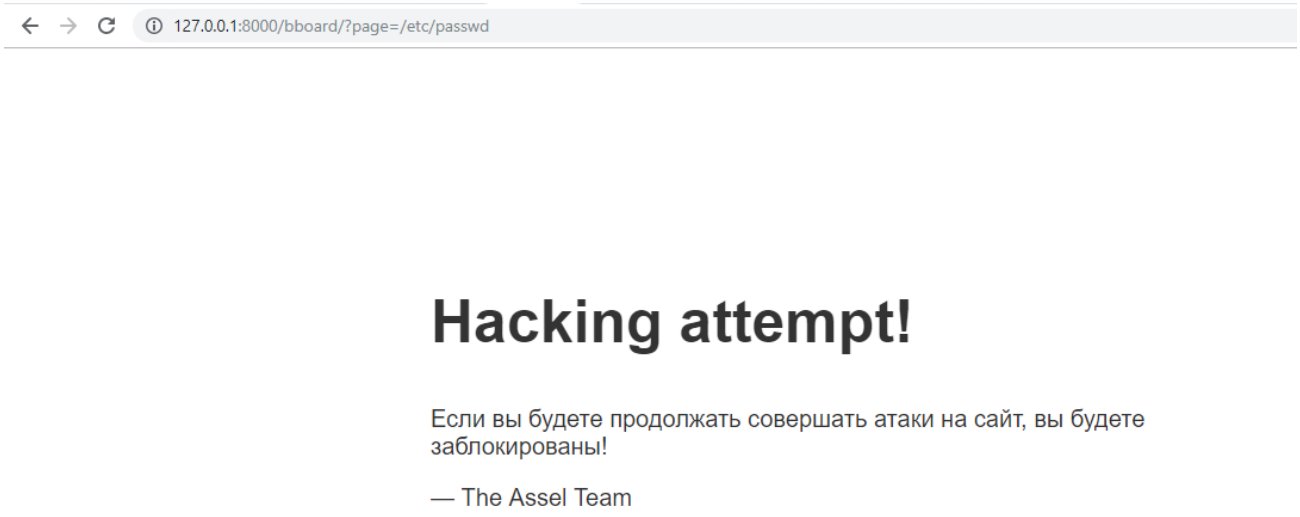
Егер модуль орнатылғанға дейін сайтта шел қойылған болса, бот веб-сайттың директориясын сканерлеу жұмысын жасайды, және шелл табылған жағдайда администарторға залалды файл анықталғаны туралы хабар жіберіледі, ол 2.17-суретте көрсетілген. Бұл веб шеллдарды табу үшін seclist-а тізімі (2.16-сурет) пайдаланылды.




Сурет 2.16 – Seclist-а тізімі




Сурет 2.17 – Администраторға келген шелл туралы хабарлама




Сурет 2.18 – Веб сайттың бұғаттауы

Рұқсатсыз басып кіруді анықтау жүйесі модулінің жұмыс принципі А қосымшасында көрсетілген.

## 3 Техникалық – экономикалық негіздеме

### 3.1 Жобаның сипаттамасы

Бұл дипломдық жобаның мақсаты ақпараттық жүйедегі рұқсатсыз басып кірулерді (шабуылдарды) анықтау жүйесін әзірлеу болып табылады.

Кәсіпорын сайтында әзірленген модульде администратор болады, ол деректерде заңсыз өзгерту кезінде шабуылдаушы журналға түседі. Администратор шабуылдаушының IP-ін бұғаттай алады немесе жүйе автоматты түрде белгілі бір мүмкіндіктерден кейін автоматты түрде бұғаттайды.

Бұл жобаны иерархиялық қағидат бойынша ұйымдастырылған мамандар тобын пайдалана отырып жүзеге асыру жоспарланып отыр. Топқа: әзірлеуші, әзірлеуші-бағдарламалаушы кіруі тиіс.

Жоба жетекшісі жұмысты орындаудың толық күнтізбелік кестесін әзірлеуге көмек көрсету және оның сақталуын бақылау, бітіру біліктілік жұмысының жоспарын жасауға көмек көрсету, әңгімелесу және консультациялар өткізу, орындалған бітіру біліктілік рботын бөліп-бөліп, сондай – ақ тұтастай тексеруге тиіс. Бағдарламалаушы-әзірлеуші теориялық негіздемені әзірлеуі, жобаны жасауы, алгоритм және интерфейстік идеологияны әзірлеуі тиіс. Осылайша, әзірлеуші-бағдарламалаушыға жоспарлау үшін жауапкершілік және жобаны іске асыру үшін жалпы жауапкершілік жүктеледі. Әзірлеуші-бағдарламалаушы жүйенің бағдарламалық модульдерін іске асыруға, жұмыс тестін жүргізуге міндетті.

Менің жұмысымда әзірлеу мен енгізудің техникалық-экономикалық негіздемесі мыналарды қамтиды:

- бағдарламаны әзірлеудің еңбек сыйымдылығын анықтау;
- бағдарламаны әзірлеуге арналған шығындарды есептеу;
- әзірленген бағдарламаның ықтимал бағасын анықтау;
- қызмет етудің әлеуметтік-экономикалық нәтижелерін бағалау.

### 3.2 Бағдарламалық өнімді әзірлеудің еңбек сыйымдылығы

Дипломдық жұмыстың осы бөлігінің мақсаты БӨ әзірлеудің еңбек сыйымдылығын анықтау, БӨ әзірлеудің желілік кестесін құру, БӨ әзірлеудің кезеңдері бойынша шығармашылық еңбектің үлес салмағын, жобалық жұмыстың өзіндік құнын бағалау, БӨ пайдасын және шарттық бағасын анықтау, жұмыстың ғылыми және ғылыми – техникалық нәтижелілігін бағалау болып табылады. Жұмыстың еңбек сыйымдылығы талдау мен зерттеулерді жүргізуге арналған уақыт нормаларына сәйкес анықталды. Әрбір жұмыс түрі бойынша кезеңдерге БӨ әзірлеу процесін бөлшектей отырып және әрбір жұмыс түрін орындаудың күтілетін еңбек сыйымдылығын анықтаймыз. Дипломдық жұмысты жүргізудің әр кезеңінде әр жұмыс түрі бойынша орындаушылардың біліктілік деңгейі анықталады (Кесте 1).

Кесте 1 – Еңбек сыйымдылығының қорытынды көрсеткіштері

| БӨ әзірлеу кезеңдері | Осы кезеңдегі жұмыс түрі | БӨ әзірлеудің еңбек сыйымдылығы, адам. х сағ. |
|---|---|---|
| 1 кезең | Міндеттер қою | 18 |
| 2 кезең | БӨ әзірлеуге техникалық тапсырманы әзірлеу және бекіту | 14 |
| 3 кезең | Қорғауды әзірлеудің белгілі әдістерімен танысу | 14 |
| 4 кезең | Техникалық тапсырманы даярлау | 20 |
| 5 кезең | Жүйені дайындауды орындау | 18 |
| 6 кезең | Кешенді қорғауды әзірлеудің әртүрлі әдістеріне талдау жүргізу | 22 |
| 7 кезең | Бағдарламалық жобаның теориялық бөлігін рәсімдеу | 18 |
| 8 кезең | Бағдарламалық жобаның тәжірибелік бөлігін әзірлеу | 24 |
| 9 кезең | Әзірлеу ортасын таңдау | 14 |
| 10 кезең | Математикалық есептеулерді әзірлеу және бағдарламаны жазу | 12 |
| 11 кезең | Жобаны іске асыру | 50 |
| 12 кезең | Сынақ тестілеу | 12 |
| 13 кезең | БӨ әзірлеу қорытындысын шығару | 14 |
| 14 кезең | Енгізу | 16 |
| 15 кезең | Тестілеу | 14 |
| Нәтижесі | Жобалық жұмысты орындаудың еңбек сыйымдылығы | 280 |

Жұмыс күнінің ұзақтығы 8 сағатқа тең. Нәтижесінде бағдарламалық қамтамасыз етуді іске асыру үшін 35 жұмыс күні қажет.

### 3.3 БӨ әзірлеуге жұмсалатын шығындарды есептеу

Өзіндік құнды есептеу БӨ әзірлеу кезінде жасалған шығыстар бойынша жүргізіледі. Жобалау жұмыстарын жүргізуге кететін шығындар өндіріс алдындағы шығындарға жатады – бұл БӨ әзірлеушілері орындайтын барлық жұмыстарға арналған бір реттік шығындар.

Шығындар өзіндік құн калькуляциясының баптарын қосу жолымен анықталады:

- материалдар;
- ғылыми және тәжірибелік жұмыстарға арналған арнайы жабдықтар;
- жалақы төлемі;
- еңбекақы төлеу қорына есептеу;

- басқа ұйымдар орындайтын жұмыстарға арналған шығындар;
- басқа шығындар;
- үстеме шығынтар.

Бұл жоба бағдарламаны әзірлеу мен сынақтан өткізуді қарастырады. Демек, қойылған мақсаттарға қол жеткізу үшін бағдарламаны әзірлеу және тестілеу шығындарын, қорытынды бағдарламаның құнын, тиісті жабдықты сатып алуды, сондай-ақ шығындардың өтелімділігін есептеу қажет. Материалдық шығындар негізгі және қосалқы шығындарға, материалдарға, энергияға және БӨ әзірлеу үшін қажетті басқа да шығындарға бөлінеді. Материалдық шығындарды есептеу 2-кестеде берілген нысан бойынша жүргізіледі.

Кесте 2 – Материалдық ресурстарға арналған шығындар

| Материал атауы | Өлшем бірлігі | Саны | Бірлік үшін бағасы, теңге | Сомасы теңгемен |
|---|---|---|---|---|
| Кеңсе қағазы | Қаптама | 3 | 1 200 | 3 600,00 |
| Блокнот | Дана | 3 | 650 | 1 950,00 |
| Қалам | Дана | 2 | 130 | 260,00 |
| Маркер | Дана | 2 | 370 | 740,00 |
| Компьютер тышқаны | Дана | 2 | 4 890 | 5 000,00 |
| Нәтижесі: | | | | 16 330,00 |

Материалдық құралдарға ($З_м$) қажетті жалпы соманы 3.1-формула бойынша есептеуге болады:

$$З_м = \sum P_i * Ц_i, \quad (3.1)$$

мұнда, $\boldsymbol{P_i}$ - материалдық ресурстың і түрінің шығысы, заттай бірліктер;

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

і – материалдық ресурстың түрі;

n – материалдық ресурстар түрлерінің саны.

Бағдарламалық қамтамасыз етуді әзірлеу үшін HP RTL8723DE ноутбук қолданылады, ноутбук қуаты қойылған міндеттерді орындау үшін жеткілікті. Бағдарламалық өнімді тестілеу үшін орнатылған операциялық жүйесі бар ДК қажет болады. Windows 7/8/10 нұсқалары. Ноутбукке сым арқылы қосылу үшін смартфон қажет. Қажетті жабдықтар мен бағдарламалық қамтамасыз етуге кететін шығындарды есептеу 3-кестеде келтірілген нысан бойынша жүргізіледі.

Кесте 3 – Жоба үшін қажетті жабдық пен БҚ шығындарын есептеу

| Материалдық ресурстың атауы | Өлшем бірлігі | Осы материалдан шығынтар саны | Бірлік үшін бағасы ,тг | Нәтижесі, тг |
|---|---|---|---|---|
| Үздіксіз қуат беру көзі | Дана | 1 | 22 490 | 22 490,00 |
| HP RTL8723DE ноутбугы | Дана | 2 | 207 000 | 414 000,00 |
| Epson L-120 принтері | Дана | 1 | 43 550 | 43 550,00 |
| Ericsson T073G модемі | Дана | 1 | 14 000 | 14 000,00 |
| Нәтижесі | | | | 494 040,00 |

Осы кестеге сәйкес жобаға материалдық шығындар 494 040,00 теңгені құрайды.

$$Зм = 16\ 330 + 494\ 040 = 510\ 370{,}00(тг)$$

Электр энергиясын тұтынатын болғандықтан, бағдарламалық қамтамасыз етуді әзірлеу кезінде электр энергиясына жұмсалатын шығындарды есептеу қажет.

1-кестеге сәйкес бағдарламалаушы үшін бағдарламалық қамтамасыз етуді әзірлеу үшін шамамен 280 сағат, ал жетекшіге 120 сағат қажет. Енді 280 сағат ішінде жұмсалатын электр энергиясының құнын (3.2) есептеу қажет (Кесте 4). Принтер үшін есептеу 20 сағат кезеңі үшін жүргізіледі, себебі принтерді үнемі пайдалану қажет емес.

$$Э = З_{эл.эн.жабд.} + З_{қос.қажет.,} \quad (3.2)$$

мұнда $З_{эл.эн.жабд.}$ – жабдықтың электр энергиясына арналған шығындары;

$З_{қос.қажет.}$ – қосымша қажеттіліктерге электр энергиясының шығындары.

Жабдық үшін қажетті электр энергиясын есептеу 3.3-формула бойынша анықталады:

$$З_{эл.эн.жабд.} = \sum \boldsymbol{W} * К_{пайда} * \boldsymbol{S} * \boldsymbol{T}, \quad (3.3)$$

мұнда, W – тұтынылатын қуат, Вт;

$К_{пайда}$ – пайдалану коэффициенті ($К_{пайда}$ = 0,7..0,9).

Кесте 4 – Электр энергиясына кететін шығындар

| Аспаптардың атауы | Қуаты, кВт | Қуат коэффициенті | Жабдықтың жұмыс жасау уақыты, сағ | ЭЭ құны тг/кВтсағ | Сомасы, тг. |
|---|---|---|---|---|---|
| Ноутбук | 0,6 | 0,7 | 280 | 23,85 | 2 804,76 |
| Модем | 0,08 | 0,8 | 280 | 23,85 | 427,39 |
| Принтер | 0,5 | 0,9 | 20 | 23,85 | 214,65 |
| Үздіксіз қуат беру көзі | 0,6 | 0,8 | 280 | 23,85 | 3 205,44 |
| Жарықтандыру | 0,3 | 0,7 | 280 | 23,85 | 1 402,38 |
| Нәтижесі: | | | | | 10 845,07 |

$$З_{эл.эн.жабд.} = 10\ 845{,}07(\text{тенге})$$

Қосымша қажеттіліктерге шығынтар электр энергиясына арналған шығынның 5% көлемінде жоғары көрсеткіш негізінде есептеледі:

$$З_{қос.қажет} = 5\% * З_{эл.эн.жабд.}, \quad (3.4)$$

(3.4) формулаға сәйкес қосымша қажеттіліктерге жұмсалатын шығындарды анықтаймыз:

$$З_{қос.қажет} = 0.05 * 10\ 845{,}07 = 542{,}25\ (\text{тенге})$$

Барлық есептеулерге сүйене отырып, электр энергиясына кететін толық шығын құрайды:

$$Э = 542{,}25 + 10\ 845{,}07 = 11\ 387{,}32\ (\text{тенге})$$

Бағдарламалық қамтамасыз етуді әзірлеу үшін бұрын көрсетілгендей, екі қызметкер қажет:

- жоба жетекшісі – жұмыс уақытын басқару, жұмыс процестерін түзету, үйлестіру, пәндік облысты зерттеу;
- бағдарламалаушы – әзірлеуші – БҚ әзірлеу, тестілеу және сүйемелдеу.

Еңбекақы төлеу шығындарының сомасын келесі (3.5) формула бойынша есептеуге болады:

$$З_{ең} = \sum ЧС_i * T_i \quad (3.5)$$

мұнда, $ЧС_i$ – і қызметкердің сағаттық ақысы, тг;

$T_i$ – модельді әзірлеудің еңбек сыйымдылығы, адам.×сағ;

і – қызметкердің санаты;

n – БӨ әзірлеумен айналысатын қызметкерлердің саны.

Жобаны іске асыру кезінде қатысушылардың жұмыс уақыты біркелкі емес, сондықтан әрбір қызметкердің сағаттық ақысы және жалпы жалақы көлемін белгілеу қажет. Қызметкердің сағаттық ақасын келесі формуламен есептеуге болады:

$$ЧС_i = \frac{ЗП_i}{ФРВ_i} \quad (3.6)$$

мұнда, $ЗП_i$ – і қызметкердің айлық жалақысы, тг;

$ФРВ_i$ – і қызметкердің айлық жұмыс уақытының қоры, сағ.

Жетекшінің айлық жалақысы 225 000 теңгеге тең және әзірлеушінің айлық жалақысы 130 000 теңгеге тең. Әр қызметкердің сағаттық ақысын (3.6) формулаға сәйкес есептейміз:

$$ЧС_{жетекші} = \frac{225\,000}{21 * 8} = 1\,278{,}41 \text{ тг/сағ},$$

$$ЧС_{әзірлеуші} = \frac{130\,000}{21 * 8} = 738{,}63 \text{ тг/сағ}$$

Жетекшінің сағаттық ақысы 1 278,41 (тг/сағ) құрайды, еңбек сыйымдылығы 120 сағатқа тең. Әзірлеушінің сағаттық ақысы 738,63 (тг/сағ), әзірлеудің еңбек сыйымдылығы 280 сағатқа тең. (3.5) формулаға сәйкес қызметкерлердің еңбекақысына арналған шығындар сомасын есептеуге болады:

$$З_{ең} = 1\,278{,}41 * 120 + 738{,}63 * 280 = 153\,409{,}2 + 206\,816{,}4 = 360\,225{,}60$$

Еңбек ақы төлеу бойынша шығындарды есептеу 5-кестеде көрсетілген.

Кесте 5 – Жалақыны есептеу

| Қызметкер санаты | Біліктілігі | БӨ еңбек сыйымдылығы, сағ. | Сағаттық ақысы, тг/сағ | Сома, тг. |
|---|---|---|---|---|
| Әзірлеуші | Бағдарламалаушы | 280 | 738,63 | 206 816,40 |
| Жетекші | Инженер–жобалаушы | 120 | 1 278,41 | 153 409,20 |
| Нәтижесі: | | | | 360 225,60 |

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

$$С_с = (ФОТ - ПО) * 0{,}095 \quad (3.7)$$

мұнда, ПО – зейнетақы қорына аударымдар, олар ФОТ 10% құрайды.

$$ПО = \mathbf{360\,225{,}6 * 0{,}1 = 36\,022{,}56} \text{ теңге}$$

$$С_с = (360\,225{,}60 - 36\,022{,}56) * 0{,}095 = 30\,799{,}28 \text{ теңге}$$

Есептеу нәтижелері 6-кестеде көрсетілген.

Кесте 6 – Әлеуметтік салықты есептеу

| Қызметкер санаты | Адам саны | Жалақы, тг | Зейнетақы аударымы, тг | Әлеуметтік салық, тг |
|---|---|---|---|---|
| Жетекші | 1 | 153 409,20 | 15 340,92 | 13 116,48 |
| Әзірлеуші | 1 | 206 816,40 | 20 681,64 | 17 682,80 |
| Нәтижесі: | | | | 30 799,28 |

Негізгі қорлар амортизациясының нормаларын ҚР Салық кодексіне сәйкес анықтау қажет. НҚ амортизациясын келесі формула бойынша анықтауға болады:

$$A_г = \frac{С_{об} * Н_а}{100} \quad (3.8)$$

мұнда, $С_{об}$ – жабдықтың құны;

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

(3.8) формуласы ноутбук үшін бір жыл ішінде амортизациялық аударымдар үшін қажетті соманы есептеуге мүмкіндік береді:

$$A_г = \frac{414\,000 * 25}{100} = 97\,500 \text{ теңге}$$

Енді әзірлеу кезеңі үшін амортизация нормасын есептеу қажет:

$$A_г = \frac{97\,500 * 35}{365} = 9\,349{,}31 \text{ теңге}$$

Осылайша, барлық жабдық үшін амортизация нормасын есептеу қажет. Есептеу нәтижелері 7-кестеде келтірілген.

Кесте 7 – Негізгі қорлардың амортизациясы

| Жабдық және БҚ атауы | Жабдық және БҚ бағасы, тг | Амортизацияның жылдық нормасы, % | Жыл ішіндегі амортизация сомасы, тг | Әзірлеу кезіндегі амортизация сомасы, тг |
|---|---|---|---|---|
| Ноутбук | 414 000 | 25 | 97 500,00 | 10 417,8 |

*7-кестенің жалғасы*

| | | | | |
|---|---|---|---|---|
| Үздіксіз қуат беру көзі | 22 490 | 25 | 5 622,50 | 539,14 |
| Модем | 14 000 | 20 | 2800,00 | 268,49 |
| Принтер | 43 550 | 25 | 10 887,50 | 1 163,30 |
| Нәтижесі: | | | 112 408,20 | 12 388,73 |

Барлық берілген есеп-қисаптардың негізінде 8-кестеде келтірілген нысан бойынша әзірлеуге арналған шығыстар сметасын ресімдеу қажет.

Кесте 8 – БҚ әзірлеуге арналған шығындар сметасы

| Шығындар баптары | Сомасы, тг |
|---|---|
| Жабдыққа кеткен шығын | 510 370,00 |
| Еңбекақы төлеу шығындары | 360 225,60 |
| Социалды налықтар | 30 799,28 |
| Электр энергиясына кеткен шығын | 11 387,32 |
| Негізгі қорлардың амортизациясы | 12 388,73 |
| Смета бойынша қорытынды: | 925 170,57 |

### 3.4 Бағдарламалық өнімнің ықтимал (шарттық) бағасын анықтау

БӨ ықтимал (шарттық) бағасының шамасы тапсырыс берушінің (тұтынушының) және орындаушының экономикалық мүдделеріне жауап беретін деңгейде оның орындалу тиімділігі, сапасы мен мерзімдері ескеріле отырып белгіленуі тиіс. Қолданбалы БӨ үшін шарттық баға (Цд) (3.9) формула бойынша есептеледі:

$$Цд = Знир(1 + Р/100), \quad (3.9)$$

мұнда, Знир – БӨ әзірлеуге жұмсалатын шығындар (8 – кестеден), тг;

Р – бағдарламалық өнімнің рентабельділігінің орташа деңгейі, % (20-30% мөлшерінде қабылданады). Бұл параметр 25% тең.

$$Цд = 925\ 170{,}57\left(1 + \frac{25}{100}\right) = 1\ 156\ 463{,}21 \text{ тенге}$$

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 құнын ҚҚС – ты ескере отырып (3.10) формула бойынша есептеуге болады:

$$Ц_р = Ц_д + Ц_д * НДС, \quad (3.10)$$

$$Ц_р = 1\ 156\ 463{,}21 + 1\ 156\ 463{,}21 * 0{,}12 = 1\ 295\ 238{,}80 \text{ тенге}$$

Бұл бағаны 1 295 240,00 теңгеге дейін дөңгелектеуге болады [9].

### 3.5 Бағдарламалық өнімнің жұмыс істеуінің әлеуметтік–экономикалық нәтижелерін бағалау

Бұл жобаның экономикалық мақсаттылығы сандық және сапалы құрамдастардан құралатын болады. Әзірлеушілер үшін экономикалық тиімділік жеке әзірлеушілер мен жобаны іске асырумен айналысатын кәсіпорындардың қаржылық жағдайын жақсартудан тұрады. Осы жобаны сәтті іске асыру кезінде әзірлеушілер 360 225,60 теңгені құрайтын жалақы алады. Әзірлеушілер үшін сапалы тиімділік-бұл жобаны нарыққа шығарудың алғашқы тәжірибесі, онда әзірлеуші одан әрі жобалау мәселелерін шешеді, жобаның тиімділігі, одан әрі жұмыс негіздерін жобалау. Сондай-ақ жобаны іске асыру барысында жарнама маркетингі, бағдарламалық қамтамасыз ету нарығын игеру мәселелері шешілетін болады. Бұл жобаның өзіндік құны 925 170,57 теңгені, пайда 231 292,64 теңгені құрады. Қорытындылай келе, осы жобаның ықтимал бағасы 1 295 240,00 теңге.

## 4 Өмір тіршілік қауіпсіздігі

### 4.1 Компьютермен жұмыс кезіндегі қауіпті және зиянды факторлар

Қазіргі кезде компьютерлеу қоғамдық өмір мен адам өмір мен адамның іс әрекетінің барлық салаларын қамтыған. Сонымен бірге, қазіргі заманғы ақпараттық технологияларды енгізу, адам ағзасына қолайсыз факторларының әсер ету мүмкіншілігінен айырылмаған болып шықты. Компьютерлермен жұмыс істейтін адамдардың қауіпсіздігін қамтамасыз ету жөнінде көңіл аударуды қажет ететін мәселе пайда болды. Бұл мәселе, компьютермен жұмыс істеуді жиі үй жағдайында да жалғастыруына және оның ұзақтығын бақылауға мүлде мүмкіншілік болмайтынына байланысты, одан да күрделене түседі.

Компьютерлермен жұмыс істеу кезінде адамға факторлардың бірқатар кешені әсер етеді, олар:

1) электромагниттік сәулеленулер:

- инфрақызыл, радиожиілік (5-тен 440 кГц дейін), ультракүлгін және рентген диапазондарындағы;
- электростатикалық өріс;
- жиілігі 50 Гц электромагниттік өріс.

2) көзге көрінетін факторлар;

3) жұмыс операцияларын орындаумен, жұмыс орнын, қимылдарды және жұмыс кезіндегі дене қалпын ұйымдастырумен байланысты факторлар;

4) микроклиматтық факторлар, ауа ортасының сапасы, жарықтану дәрежесі;

5) шу, діріл.

Факторлардың бірінші екі тобының әсер ету қарқындылығы мен сипаты көбіне мониторлардың түріне байланысты: ол электронды-сәулелі түтікті ме (ЭСТ), сұйық кристаллды ма (СК), плазмалық па немесе басқа түрлері ме. Электронды сәулелі түтікті мониторлардағы электромагниттік сәулелену көздеріне дисплей схемасының жоғары вольтты элементтері, электронды-сәулелі түтік және монитордың экраны жатады. Дисплейден сәулеленетін радиожиілік диапазонындағы электромагниттік өріс 5 Гц-тен 400 кГц дейінгі жиілікте болады, соған байланысты толқын ұзындығы да үлкен болады, сондықтан да экран алдында жұмыс істейтіндерге электрлік және магниттік құрамдастары жеке-жеке әсер етеді. Ол жұмыс орындарының индукция зонасында, яғни қалыптаспаған магнитті өрісте болуымен түсіндіріледі, себебі толқын ұзындығы өте үлкен, бірнеше жүздеген метрлерге дейін жетеді, ал индукция зонасыгың шегарасы шамамен толқын ұзындығының 1/6 бөлігіне тең аралықты қамтиды.

Бейнедисплейлік терминалдардан шығатын радиожиілікті электромагниттік өрістің, ультракүлгін, инфрақызыл сәулеленулердің және электростатикалық өрістің қарқындылығы төмен болады, әдетте экраннан 30-50 см қашықтықта олардың деңгейі ШРЕД-тен аспайды. Сонымен бірге, электронды сәулелі түтікті мониторлармен жұмыс істегенде 2-6%

жағдайларда электростатикалық өрістің кернеулілігі ШРЕД-тен 2-20 есеге дейін, ал 9-15% жағдайларда электромагниттік өрістің электрлік құрамдасы ШРЕД- тен 4-тен 10 есеге дейін, магниттік құрамдасы ШРЕД-тен 1,5 есе артық болғаны да байқалады.

### 4.2 Компьютерден бөлінетін сәулелердің адам ағзасына 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.

Жүйке жүйесіне әсері. Тіпті жылулық әсер байқалмайтын электромагнитті сәулелену деңгейі ағзаның ең маңызды деген қызметтік жүйелеріне әсер етеді. Осы саладағы мамандардың көпшілігінің ойынша жүйке жүйесі ең осал ағза болып табылады. Әсер ету механизмі өте қарапайым – анықталған, электромагнитті өріс кальций иондары үшін торлы мембрана өткізгіштігін бұзады. Нәтижесінде жүйке жүйесі қалыпты қызметінен ауытқи бастайды. Аталған процесстер барысында туындайтын ауытқулар ауқымы кең – жүргізілген тәжірибелер барысында есте сақтау қабілетінің төмендеуі, реакцияның төмендеуі, депрессиялық өзгерітер және т.б. сынды құбылыстар тіркелген.

Имундық жүйеге әсері. Имундық жүйеде әсер ету аймағына ұшырайды. Бұл бағыттағы тәжірибелік зерттеулер ЭМС сәулелендірілген жануарларда

инфекциялық процесс сипаты өзгеретінін көрсеткен ( инфекциялық процесстің жүруі ауырлайды).

ЭМС әсер еткен кезде соңы жойылуға әкеп соғатын иммуногенез процессі бұзылады. Бұл процессті аутоиммунитет туандауымен байланыстырады.

Жоғары қарқындылықтағы электромагниттік өрістің ағзаның имун жүйесіне әсері имунитеттің торлы Т-жүйесінің жойылу эффектісінен байқалады.

Эндокринді жүйеге әсері. Эндокринді жүйе де электромагниттік сәулеленуге ұшырайды. Зерттеулер электромагниті өрістің әсер етуі кезінде гипофизарлы-адреналинді жүйенің стимуляциясы болатынын және ол қандағы адреналин көлемінің артуымен қатар жүретінін көрсетті.

Жүрек қан тамырлар жүйесіне әсері. ЭМӨ әсер ету нәтижесі ретінде жүрек қан-тамырлар жүйесі қызметінің бұзылуын қарастыруға болады. Ол артерия қысымының және тамыр соғысының тұрақсыздығынан байқалады. Периферлік қан құрамының фазалық өзгеруі белгіленеді.

Жыныс жүйесіне әсері. Туа бітті кемтарлық пен кемістік жағдайларының көбеюі, қыз жынысты балалардың дүниеге келу ықтималдығының артуы, спермакинездің жойылуы байқалады.

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

### 4.3 Компьютерден бөлінетін сәулелерден қорғану 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.

### 4.4 Электро-магниттік өрістің әсерінен қорғану

Жеке адамдық компьютерлердің (ЖАК) электромагниттік өрісі адам ағзасына қолайсыз әсер етуі мүмкін. Бұл сәулеленулер ағзадағы сұйықтықтардың құрамын өзгертіп және ағзаға бірқатар минералды заттардың қажеттілігін өзгертіп, адам ағзасындағы биологиялық үрдістерге әсер ететінің, зерттеулер көрсетіп отыр. Бұл кезде бір шұғыл ағзадан шығуы жоғарласа заттардың жоғарласа (Ca, Ba, Al), басқаларының шығуы шұғыл азаяды (Fe, P), яғни минералдардың алмасуында белгілі бір бұзылыстар жүреді. Бұл жеке адамдық компьютерледің ЭМӨ-нің жасуша мембраналарының иондық өзекшелеріне тікелей әсер етуімен, немесе гормондары минералды заттардың алмасуына бүрек үсті безінің белсенділігі артуымен түсіндіріледі.

Айнымалы электромагниттік өріс елеулі физиологиялық реакция тудыратыны және ағзаның иммунды, жүйке және жүрек-қантамыр жүйелерінде және көру анализаторларында бұзылулар пайда болуына әкеп соғатыны белгілі. Компьютермен ұзақ жұмыс істегенде астениялық, астено-невроздық синдромдар, вегетотамырлық дисфункция дамиды. Бас ауруы, ашушаңдық, тез қажығыштық, ұйқысының бұзылуы негативті эмоционалдық жағдайлар (жиі депрессия) байқалады. Еңбекке қабілеттілігі, ақпараттарды қабылдау және өндеу жылдамдығының, есте сақтау қабілетінің төмендеуі байқалады. Жүрек тұсының ауруы, брадикардия, ангиоспастикалық реакциялармен ауысып отыратын артериалды қан қысымның төмендеуі жиі кездеседі. Эндокриндік жүйеде, зат алмасуында бұзылулар болуы, атап айтқанда қалқанша безінің белсенділігінің төмендеуі мүмкін.

Электростатикалық өрістің биологиялық әсері негізінен астено-невроздық синдром мен вегетотамырлық дистония түріндегі қайтымды функционалдық өзгерістерімен білінеді. Мұнан басқа, электросатикалық өріс микробөлшектерді, шаң бөлшектерін «зарядтайтын» және олардың қонуына кедергі келтіретін қабілеті бар, соған байланысты мұндай шаң «коктейлімен» тыныс алу теріде, көзде, жоғарғы тыныс жолдарында және басқаларда аллергиялық аурулар дамуына алып келеді. Мысалы, дисплейлермен күніне 2-

6 сағат және одан да артық уақыт жұмыс істегенде, экземамен ауру қаупі жоғарлайтыны туралы мәліметтер бар.

Электромагниттік сәулелену дегеніміз-электромагниттік өрістердің кеңістіктегі жағдайының өзгерісі.Магнит және электр өрістерінің кез келген өзгерістері қоршаған кеңістікті сүзіп өтетін күш сызықтарының өзгеруін туындатуы керек, яғни ортада таралатын импульстар (немесе толқындар) болу керек. Осы толқындардың таралу жылдамдығы ортаның магниттік және диэлектриктік өтімділігіне тәуелді болып, электромагниттік бірліктің электростатикалық бірлікке қатынасымен анықталады. Компьютерлік техниканың пайда болуымен қарыштап дамуы қоршаған ортада электромагниттік ахуалдың өзгеруіне алып келді. Компьютерлік техника электромагниттік өрістің сәулелену көзі болып табылады, ал ол өз кезегінде адам денсаулығына қауіп төндіретіні белгілі. Компьютерлік жұмыс орындарының дұрыс ұйымдастырылмауы электромагниттік өрістің адам денсаулығына кері әсер етуіне әкеліп соғады. Компьютердің ең қауіпті бөлігі-монитор.Ол адам ағзасын сәулелендіреді. Медицина өкілдерінің зерттеулері электромагниттік өрістің әсері метаболизм мен электромагниттік бұзылуынаықпал ететіні дәлелденген. Ол сонымен қатар жүйке жүйесі, жүрек қан тамырлары, эндокринді жүйе жұмысында да пайда болуына әсер етеді.Қалта телефонын пайдаланған кезде одан бөлінетін электромагниттік өріс тұтынушының миына әсер ететіні анықталған. Электромагниттік сәуледен адамға әсер ету деңгейі сәуленің интенсифтілігіне, жиілігіне және әсер ету уақытына байланысты. Үлкен интенсифтік өрістің адамға ұзақ уақыт әсер беруі адамның күйзелу күйіне, шаршаңқы болуына,ұйқыға әуестігіне, ұйқының бұзылуына, бастың ауыруына, гипертонияға, жүрек тұсындағы ауырлыққа әкеліп соқтырады. Өте жоғары жиілікті өрістің әсері адамның қан құрамының өзгерісіне,көздің ауруына әсер етеді. Электромагнитік өрістің әсері - электр заряды не магниттік моменті бар бөлшектер арасындағы электромагнитік өріс арқылы берілетін белгілі. Адам өмірге келгеннен бастап, электромагнит сәулесінің әсерінде болады. Адамға әсер ететін жердің магниттік өрісі - табиғи электромагниттік өріс, планетарлық сарқылмайтын ресурс. Магниттік өрістің күші әржерде әртүрлі. Радиожиіліктік өрістер адам организіміне қолайсыз әсерін тигізеді. Адамға, жануарларға, өсімдіктерге, микроорганизмдерге жер қыртысынан бөлінетін гамма сәулелер және ғарыш сәулелері сырттан,организмде болатын радиоактивті элементтер сәуелері іштен әсер етеді. Егер бұл сәулелер тірі организмге артық мөлшерде өтсе, клеткалардың, органдардың тіршілігіне қауіпті ауру жабысады. Радиожиілікті қондырғылар шығаратын электромагниттік сәулелерді мөлшерден көп қабылдаған жағдайда ол адамда мамандық ауруға әкеліп соғады. Нәтижесінде нерв жүйесі журек қан тамырлары эндокриналды жүйе және де басқа да ағзаларға әсер етуі мумкін. Электромагниттік өріс әсерінде ұзақ уакыт болған жағдайда адамдар тез шаршайды. Ұйқышылдық пайда болады,ұйқысы бұзылады, жиі-жиі басы ауырады, нерв жүйесі бұзылады т.с.с. системетикалық сәулелену болған жағдайда психикалық ауру қан қысымы

өзгеру жүрек соғысының баяулауы шашының түсуі байқалады. Қорғану әдістері: сәуле шығару көзіндегі сәулеленуді азайту. Өте жоғары жиілікті және ультра жиілікті қондырғыларды дұрыс орнату. Экрандалған бөлмелердегі қондырғыны алыстан бақылау. Жұмыс істеу орнын және сәуленің шығу көзін экрандау немесе мыстан жасалтын жогары өткізгіштік қасиеті бар тор металдар шағылдырғыш жерлету экран ретінде пайдалану шаралар электормагниттік сәулеленуді дозиметр көмегімен кемінде айына бір рет тексеру, жылына медициналық тексеруден бір рет өткізу. Қосымша демалыс қысқартылған жұмыс күнін жасау жасы он сегізге толмаған және орталық нерв жүйесі жүрегі, көзі ауыратын тұлғаларды жұмысқа қабылдамау.

Иондаушы сәулелер әсерінің ерекшеліктері келесідей сипатталады:

- адам сәуленің организмге әсерін сезбейді (адамдар иондаушы сәулелерді қабылдайтын сезім мүшелеріне ие емес);
- иондаушы сәулелер адам денсаулығына зиянды әсерін тигізеді (сондықтан кез келген иондаушы сәулелерді қауіпті деп қараған жөн);
- адам организмінің жеке ерекшеліктері радиацияның аздаған мөлшерінде пайда болады (адам неғұрлым жас болса, соғұрлым сәулеленуге сезімтал болады, 25 жастан бастап адам сәулеленуге тұрақты бола бастайды);
- адам неғұрлым көп мөлшерде сәуле ауруының нышаны, бірақ аурудың нышаны біраз уақыт өткеннен кейін ғана байқалады;
- сәулелену мөлшері жасырын түрде жинақталады (сәулелену мөлшері уақыт өткен сайын жинақталып, сәуле ауруына ұшыратады).

Радиациядан қорғанудың үш әдісі бар-олар:

- уақытпен қорғау;
- қашықтықпен қорғау;
- экрандау және жұтып алу арқылы қорғау.

Уақытпен қорғау-радиобелсенді заттармен ластанған объектіде немесе жергілікті орында адамдардың болуы уақытын шектеу неғұрлым болу уақыты аз болса, соғұрлым қабылданған мөлшер де аз болады. Қашықтықпен қорғау-радиация деңгейі жоғары немесе жоғарылауы мүмкін жерлерден адамдарды эвакуациялау. Экрандау және жұтып алу арқылы қорғау-адамдарды эвакуациялау мүмкін болмаған жағдайда қолданылатын әдіс.Бұл әдіспен қорғауда панаханалар, жасырыну орындары және жеке қорғаныс құралдары қолданылады. Тұрғындарды, радиобелсенді заттармен залалдану туралы, төтенше жағдайлар министрлігінің азаматтық қорғаныс (АҚ) органдары хабардар етеді. Жергілікті аймақтың (ауданның) радиобелсенді залалдануы басталған кезінде немесе бірнеше сағатта басталуы мүмкін кезінде Радиациялық қауіп дабылы соғылады. Дабыл жергілікті радио немесе теледидар желілері арқылы жеткізіледі.Радиациялық қауіп туралы естіген тұрғындар, тез арада бұқаралық ақпарат құралдары бойынша алынған ұсыныстарға сәйкес іс-қимыл жасауы керек. Радиациялық сәулелену адам ағзасына (қан айналымы ,жүйке жүйесіне, асқазанына) және оның дамуына иондық сәулелердің өтуімен кері әсерін тигізеді. Радиоактивті заттардың ағзаға әсерін әлсірету үшін:

- ғимараттан қажетілігі болмаса шықпаңыз, шыққан жағздайда респиратор, плащ, резенке етік жіне қолғап киіп шығыңыз;

- ашық ортада шешінбеңіз, отырмаңыз, темекі шекпеңіз, ашық су аумағында суға түспеңіз, саңырауқұлақ, жеміс-жидектер жинамаңыз;

- ғимаратқа кірер алдында аяқ киіміңізді жуып, сыртқы киіміңізді қағып, сүртіп киіңіз;

- суды тек таза тексерілген көздерінен алып, ал азық түлікті дүкендерден сатып алыңыз;

- тамақ ішер алдында қолыңызды, ауызыңызды 0,5 пайыздық ерітіндідегі ас содысымен шайып жуыңыз. Осы берілген мағлұматтар сәулелену ауруынан алдын алуына көмектеседі.

Төменде көрсетілген сыртқы сәулеленуден қорғану әрекеттерінің негізі болатын-гамма сәулеленудің қайнар көзі рентгендік және нейтрондық сәулеленулермен жұмыс жасағанда да таралады:

- радиоактивті әртүрлі газ;

- сыртқы ортаның ластанған объектілерінің әсер ететін сәулесі; -тыныс алу жолында, терідегі жіне көздің сыртқы кабыршағында радиактивті заттардың болуы;

- құрамында нуклидтер бар ауа, тамақты қолданғанда;

- рентгендік және кейбір нейтрондық сәулеленудің қайнар көздері тек өздеріне тән құралдардың іске қосылуымен ғана әсер береді;

- сөндірілген құралдар сәулеленудің қайнар көзі болып табылмайды. Ионданған сәулелер адам, жануар организмдерінде ақуыз, фермент және басқа да заттардың өзгеруіне, яғни сәуле ауруының дамуына әкеліп соғады [10].

## Қорытынды

Ақпараттық жүйелердің компоненттеріндегі осалдықтар болмаса да, көптеген шабуылдарды іске асыруға болмайды, демек, дәстүрлі қорғаныс жүйелері ықтимал шабуылдарды тиімді түрде жеңе алар еді. Бірақ бағдарламалар қателіктер жасауға тән адамдар жазады. Осының салдарынан шабуылдарды іске асыру үшін зиянкестер қолданатын осалдықтар пайда болады. Егер барлық шабуылдар «бір-біріне» үлгісі бойынша салынса, онда кейбір тартумен, бірақ желіаралық экрандар мен басқа да қорғаныс жүйелері оларға қарсы тұра алатын еді. Бірақ, дәстүрлі қаражат тиімсіз болатын Үйлестірілген шабуылдар пайда болды. Сондықтан жаңа технологиялар пайда болады - шабуылдарды анықтау технологиясы. Келтірілген жүйелеу шабуылдар және оларды іске асыру кезеңдері туралы деректер шабуылдарды анықтау технологияларын түсіну үшін қажетті базис береді. Шабуылдарды анықтау жүйесі-бұл ұйымды қорғаудың тиімді жүйесін қамтамасыз ету үшін қажетті, бірақ жеткіліксіз жағдай. Шабуылдарды анықтаудың тиімді және сенімді жүйесі орталық консольде көптеген қашықтағы Сенсорлардан ақпаратты жинауға, жинақтауға және талдауға мүмкіндік береді. Ол бұл ақпаратты кейінірек талдау үшін сақтауға мүмкіндік береді және мұндай талдау жүргізу үшін қаражат береді. Бұл жүйе үнемі барлық орнатылған бақылау модульдерін бақылайды және дабыл пайда болған жағдайда дереу жауап береді. Шабуылдарды анықтау жүйесі, егер штатта ақпаратты қорғау саласындағы сарапшылар болмаса, бұл жүйені қалай пайдалану және үнемі өсіп келе жатқан ақпараттық қауіпке қалай әрекет ету керектігін білетін қымбат ойыншықтан артық емес. Барлық осы компоненттерді кешенді пайдалану шабуылдарды анықтаудың нақты және тиімді жүйесін құрайды.

Қазіргі ақпараттық технологияның дамыған заманында, ақпараттық технологиялардың мүмкіндігін пайдаланушы қылмыстық топтар әр түрлі кәсіпорындардың маңызды ақпараттарына шабуыл жасауда. Нақтылап айтар болсақ, компьютерлік жүйелерден ақпараттарды ұрлау, оларды заңсыз және күшпен иемденіп алу, ақпарат қорларына қашықтан шабуыл жасауды ұйымдастыру, ақпаратты жоюды, жинау және өзгертуді мақсат ететін компьютерлік вирустарды жасап, олардың көмегімен шабуылдар ұйымдастыру. Олардың қатарында «логикалық бомбалар», «троняндық коньдар», «инъекциялар», т.б. көптеген ақпараттық қарулар бар.

Компьютерлік жүйеге жасалып жатқан кез келген шабуыл желілік трафикті немесе желілік ресурстарды талдау барысында анықталады.

Бұл дипломдық жобада «Trassir» компаниясының сайтына жасалған рұқсатсыз басып кірулерді (шабуылдарды) анықтау жүйесінің модулі әзірленген. Пайдаланушыдан серверге жіберілген сұраныстарды алдымен модуль өңдейді. Python бағдарламалық тілінде жазылған бағдарлама арқылы модуль сұранысты белгілі бір ережеге сәйкестігі бойынша тексереді. Талдау нәтижесіне байланысты, күдікті пайдаланушыларға жауап қайтармайды немесе оларды бұғаттайды.

## Қысқартулар тізімі

АҚ – ақпаратты қорғау
АЖ – ақпараттық жүйе
ТЖ – технология жүйесі
АТ – ақпараттық технологиялар
ДК – дербес компьютер
БҚ – Бағдарламалық қамтамасыз ету
БӨ – бағдарламалық өнім
ҚҚС – қосылған құн салығы
АҚЖ – ақпаратты қорғау жүйесі
НЖ – нейрондық желілер
ДБ – деректер базасы
ОЖ – операциялық жүйелер
ЖЭ – желіаралық экран
HTML (Hypertext Markup Language) – вебшолғышта көрсетілуге арналған еренмәтін мен басқа ақпараттардан тұратын веб-парақшаларды жасауға арналған белгілеу тілі
HTTP (HyperText Transfer Protocol) – интернетте HTML беттерін алмасу үшін арналған хаттама
SQL (Structured Query Language) – реляциялық дерекқорларын құруға, өзгертуге және басқаруға арналған универсалды компьютер тілі
URL (Uniform Resource Locator) – интернеттегі қор көзін бірегей түрде айқындайтын мекенжай

## Әдебиеттер тізімі

1 Платонов В. Программные-аппаратные средства защиты информации. -М.: Академия, 2013

2 Лукацкий А.В. Обнаружение вторжений. -СПб.:БХВ-Петербург, 2001

3 Милославская Н.Г., Толстой А.И. Интрасети: Обнаружение вторжений. -М: Юнити, 2001

4 Акбарова Ш.А., Ганиев А.А. Классификация IDS // «Молодой ученый» №15 (149), сәуір 2017

5 Васильев В.И., Свечников Л.А. Архитектура респределенной сети обнаружений вторжений. -Таганрог: Изд-во ТРТУ, 2006

6 Васильев В.И., Свечников Л.А. Способ реализации нейросетевого датчика интеллектуальной системы обнаружения атак. -Уфа: Изд-во УГАТУ, 2006, -С.161-166.

7 Свечников Л.А. Моделирование и оптимизация системы обнаружения атак в локальных вычислительных сетях. -Таганрог: Изд-во «Технология», 2007

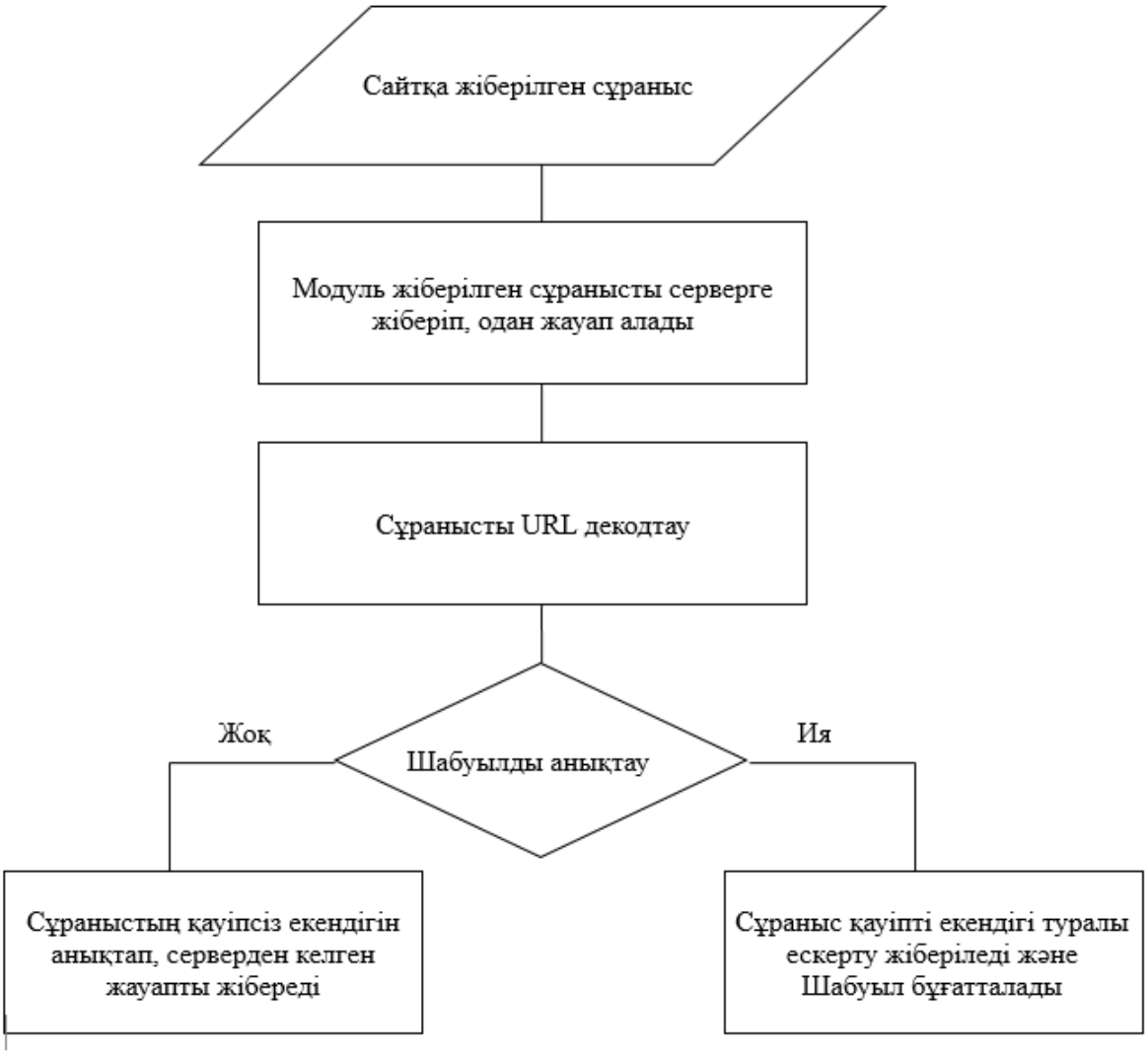
8 Чан У, Биссекс П., Форсье Д. Django. Разработка веб-приложений на Python [Электронды ресурс]- ISBN 978-5-93286-167-7, Изд-во "Символ-Плюс", 2009

9 Бекишева А.И. Методические указания к выполнению экономической части диломной работы для бакалавров специальности 5В0703 - Ифнормамционные системы - Алматы: АУЭС, 2013. -24с.

10 Вербецовский А.А. Основы компьютерных технологий и современные ПК. -М.: АЛЕКС, 2002. -264 с.

## А қосымшасы

## Модельдің жұмыс жасау принципі



## Б қосымшасы

## Бағдарлама листингі

```
import re
import urllib.parse
from django.http import HttpResponse
import datetime
def urldecode(str):
return urllib.parse.unquote(str)
rules=['select',
'etc',
'passwd',
'script',
'order',
'ls -l',
'rm -rf',
'/../../',
'{{',
'}}',
'group+by',
'concat',
'php:',
'base64',
'@import',
%(HOME(DRIVE|PATH)|SYSTEM(DRIVE|ROOT)|WINDIR|USER(DOMAIN|P
ROFILE|NAME)|((LOCAL)?APP|PROGRAM)DATA)%',
'bunionb.+?bselectb',
'{{([a-zA-Z]{50})}}',
'group by ([\d]){2}',
'order by ([\d]){2}',
'type=\"text/javascript\"',
'onerror=\"javascript',
'<a href=\"javascript\\']
def StatisticsMiddleware(get_response):
def middleware(request):
response = get_response(request)
# Code to be executed for each request/response after
# the view is called.
a=request.META
print(a['QUERY_STRING'])
#int('Attacker\'s ip:'+a['REMOTE_ADDR']+'  '+'request
method:'+a['REQUEST_METHOD']+'  '+'user agent:'+a['HTTP_USER_AGENT'])
for n,rule in enumerate(rules):
if re.search(rule,urldecode(a['QUERY_STRING'].lower()))!=None:
```

```
with open(r"test.txt", "a") as file:
file.write('Attacker\'s ip:'+a['REMOTE_ADDR']+','+'request
method:'+a['REQUEST_METHOD']+','+'payload:'+a['QUERY_STRING']+','+'user
agent:'+a['HTTP_USER_AGENT']+',time:'+'{}'.format(datetime.datetime.now())+'\
n')
return HttpResponse('''<!doctype html>
<title>Site Maintenance</title>
<style>
body { text-align: center; padding: 150px; }
h1 { font-size: 50px; }
body { font: 20px Helvetica, sans-serif; color: #333; }
article { display: block; text-align: left; width: 650px; margin: 0 auto; }
a { color: #dc8100; text-decoration: none; }
a:hover { color: #333; text-decoration: none; }
</style>
<article>
<h1>Hacking attempt!</h1>
<div>
<p>Если вы будете продолжать совершать атаки на сайт, вы будете
заблокированы!</p>
<p>&amp;mdash; The Assel Team</p>
</div>
</article>''')
#print(n)
 #print(len(rules))
 if n==(len(rules)-2):
print(10)
return response
return middleware
```

**Бот листингі**

```
import re
import time
import telebot
from telebot import types
from telebot.types import Message
import os
token='666593482:AAFikdCnp7GJ5Zs-yfGSHSXMWRcs-4-wngw'
global url
url=''
bot=telebot.TeleBot(token)
import telebot
shells=['c99.php',
'c99shell.php',
```

'r57.php',
'r58.php',
'dra.php',
'r00t.php',
'root.php',
'mma.php',
'filesman.php',
'Locus7s.php',
'c99-Ultimate.php',
'c100.php',
'Ekin0x.php',
'hacker.php',
'safe0ver.php',
'sniper.php',
'spyshell.php',
'CWShellDumper.php',
'angel.php',
'dq.php',
'cmd.php',
'liz0zim.php',
'simattacker.php',
'tryag.php',
'150.php',
'Ani-Shell.php',
'Crystal.php',
'Dx.php',
'FaTaLisTiCz_Fx.php',
'G5.php',
'NCC-Shell.php',
'NetworkFileManagerPHP.php',
'PHANTASMA.php',
'PHPJackal.php',
'PHPRemoteView.php',
'PHPSPY.php',
'Php_Backdoor.txt.php',
'Private-i3lue.php',
'SnIpEr_SA Shell.php',
'upl0ader.php',
'acid.php',
'antichat.php',
'shell.php',
'udp.php',
'ddos.php',
'b37.php',

```
'backupsql.php',
'bdotw44shell.php',
'bug.php',
'c37.php',
'c66.php',
'c99-shadows-mod.php',
'c99_Psych0.php',
'c99_locus7s.php',
'c99_madnet.php',
'c99_w4cking.php',
'c99madshell.php',
'c99ud.php',
'c99unlimited.php',
'c99v2.php',
'cbfphpsh.php',
'cihshell_fix.php',
'co.php',
'connect-back.php',
'cpg_143_incl_xpl.php',
'ctt_sh.php',
'cybershell.php',
'egy.php',
'erne.php',
'ex0shell.php',
'g00nv13.php',
'hkrkoz.php',
'ironshell.php',
'isko.php',
'iskorpitx.php',
'itsecteam_shell.php',
'locus.php',
'log.php',
'simple_cmd.php',
'zacosmall.php']
with open('test.txt') as f:
x = sum(1 for _ in f)
@bot.message_handler(commands=['start'])
def command_handler(message:Message):
while True:
with open('test.txt') as f:
z = sum(1 for _ in f)
if z>x:
with open('test.txt') as f:
lines = f.readlines()
```

```
for i in range(z-x):
bot.send_message(message.chat.id,lines[len(lines)-(i+1)])
time.sleep(60)
for root, dirs, files in
os.walk("/home/light/ProgrammsProjects/PycharmProjects/djjjjnn/"):
for file in files:
if file.endswith(".php"):#and os.path.join(file)==[i for i in shells]:
bot.send_message(message.chat.id,"На вашем сервере был обнаружен
шелл:"+(os.path.join(file)))
print(os.path.join(root,file))
if __name__=='__main__':
bot.polling(none_stop=True)
```