ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Автоматика және ақпараттық технологиялар институты

Киберқауіпсіздік, ақпаратты өңдеу және сақтау кафедрасы

Кадекешов Бекзат Тулебайулы

Компанияның ақпараттық қауіпсіздігінің кешенді жүйесін құру

ДИПЛОМДЫҚ ЖҰМЫС

5В070300 – «Ақпараттық жүйелер» мамандығы

Алматы 2022

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Автоматика және ақпараттық технологиялар институты

Киберқауіпсіздік, ақпаратты өңдеу және сақтау кафедрасы

ҚОРҒАУҒА ЖІБЕРІЛДІ
КАОжС кафедрасы меңгерушісі
т.ғ.к, қауым. профессор
_____Р.Ж.Сатыбалдиева
«__» _____2022 ж.

ДИПЛОМДЫҚ ЖҰМЫС

Тақырыбы: «Кәсіпорында ақпараттық қауіпсіздіктің кешенді жүйесін құру»

5В070300 – «Ақпараттық жүйелер» мамандығы

Орындаған: Кадекешов Бекзат Тулебайулы

Рецензент
PhD докторы, ҚР БҒМ ҒК АЕТИ АҒҚ
_____ Усатова О.А.
«18» қаңтар 2022 ж.

Ғылыми жетекшісі
Ph.D докторы, қауым. профессор
_____ Бегимбаева Е.Е.
«18» қаңтар 2022 ж.

Алматы 2022

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Автоматика және ақпараттық технологиялар институты

Киберқауіпсіздік, ақпаратты өңдеу және сақтау кафедрасы

5В070300 – Ақпараттық жүйелер

БЕКІТЕМІН
КАӨжС кафедрасы меңгерушісі
т.ғ.к, қауым. профессор
_____Р.Ж.Сатыбалдиева
«19» мая 2022 ж.

Дипломдық жұмысты орындауға
ТАПСЫРМА

Білім алушы: Кадекешов Бекзат Тулебайулы
Тақырыбы: «Кәсіпорында ақпараттық қауіпсіздіктің кешенді жүйесін құру»
Университет Ректорының 2021 жылғы «24» желтоқсан №489-б бұйрығымен бекітілген.
Орындалған жұмыстың өткізу мерзім 24.05.2022 ж.
Дипломдық жұмыстың бастапқы мәліметтері: тақырып бойынша әдебиеттерге шолу нәтижелері, теориялық мәліметтердің жиыны.
Дипломдық жұмыста қарастырылатын мәселелер тізімі:

a) Ақпараттық қауіпсіздік түсінігіне теориялық зерттеулер жүргізу;
b) Оның кәсіпорында саласында қолдану ерекшеліктері анықтау;
c) Бағдарламалық-аппараттық құралдарына сипаттама жасау;
d) Ақпаратты қорғау әдістерін талдау;
e) Диплом жұмысы бойынша қосымша әзірлеу.

Графикалық материалдардың тізімі (міндетті түрде қажет сызбалар көрсетілген): жұмыстың ____ слайдтан тұратын презентациясы көрсетіледі.
Ұсынылған негізгі әдебиет 34 кітаптан тұрады.

Дипломдық жұмысты даярлау

КЕСТЕСІ

Бөлім атауы, карастырылатын мәселелер тізімі	Ғылыми жетекші мен кеңесшілерге көрсету мерзімі	Ескерту
1. Ақпараттық қауіпсіздік түсінігіне теориялық зерттеулер жүргізу;	13.02.2022	орындалды
2. Оның кәсіпорында саласында қолдану ерекшеліктері анықтау;	05.03.2022	орындалды
3. Бағдарламалық-аппараттық құралдарына сипаттама жасау;	01.04.2022	орындалды
4. Ақпаратты қорғау әдістерін талдау;	20.04.2022	орындалды
5. Диплом жұмысы бойынша қосымша әзірлеу	04.05.2022	орындалды

Дипломдық жұмыс бөлімдерінің кеңесшілері мен норма бақылаушының аяқталған жұмысқа қойған

қолтаңбалары

Бөлімдердің атауы	Кеңесшілер (аты-жөні, тегі, ғылыми дәрежесі, атағы)	Қол қойылған мерзімі	Қолы
Негізгі бөлім	Бегимбаева Е.Е. (Ph.D докторы, қауым. профессор)	10.05.2022	
Норма бақылаушы	Аристомбаева М.Т. (Техн.ғылым. магистрі, лектор)	17.05.2022	

Ғылыми жетекшісі _____ Бегимбаева Е.Е.

Тапсырманы орындауға қабылдаған білім алушы _____ Кадекешов Б.Т.

Күні «19» ноябрь 2022 ж.

АҢДАТПА

Дипломдық жұмыс 30 беттен, 13 суреттен және 34 пайдаланылған әдебиеттер тізімінен тұрады.

Зерттеу объектісі: компания қауіпсіздігінің кешенді жүйесі.

***Дипломдық жұмыстың мақсаты*:** компанияның ақпараттық қауіпсіздігінің кешенді жүйесін жобалау.

Зерттеудің міндеттері:

- ақпараттық қауіпсіздік түсінігіне теориялық зерттеулер жүргізу;
- оның кәсіпорында саласында қолдану ерекшеліктері анықтау;
- бағдарламалық-аппараттық құралдарына сипаттама жасау;
- ақпаратты қорғау әдістерін талдау;
- диплом жұмысы бойынша қосымша әзірлеу.

Мәселені талдау дәрежесі. Дипломдық жұмыстың тақырыбын зерттеу барысында отандық және шетелдік ғылыми еңбектері мен оқулықтар, электронды басылымдардағы ғылыми мақалалар қолданылды.

Жұмысты орындау барысында компьютерлік технологиялар қолданылды, атап айтқанда мәліметтер базасы Python ортасында құрастырылып, қолданушының интерфейсі Django визуалдық компоненттері арқылы жүзеге асырылған. Сондай-ақ жұмыста отандық және шетелдік ғалымдардың еңбектері мен мақалалары қолданылды.

Дипломдық жұмыстың қолданылу аясы: алынған нәтижелерді зерттеу мақсатында, сонымен қатар қоғамда, шағын және орта бизнес субъектілері жұмысы үшін қолданылады.

АННОТАЦИЯ

Дипломная работа состоит из 30 страниц, 13 рисунков и 34 списков использованной литературы.

Объект исследования: комплексная система безопасности компании.

Цель дипломной работы: проектирование комплексной системы информационной безопасности компании.

Задачи исследования:

- проведение теоретических исследований понятия информационной безопасности;
- выявить особенности его применения на предприятии;
- разработка описания программно-аппаратных средств;
- анализ методов защиты информации;
- разработка приложения по дипломной работе.

Степень анализа проблемы. При изучении темы дипломной работы использовались отечественные и зарубежные научные труды, учебники, научные статьи в электронных изданиях.

При выполнении работы были использованы компьютерные технологии, в частности, база данных была скомпилирована в среде Python, а пользовательский интерфейс реализован через визуальные компоненты Django. Также в работе использованы труды и статьи отечественных и зарубежных ученых.

Область применения дипломной работы: используется в целях изучения полученных результатов, а также в обществе, для работы субъектов малого и среднего бизнеса.

ANNOTATION

The thesis consists of 30 pages, 13 drawings and 34 references.

The object of research: the company's integrated security system.

The purpose of the thesis: designing a comprehensive information security system of the company.

Research objectives:

- conducting theoretical studies of the concept of information security;
- to identify the features of its application in the enterprise;
- development of a description of software and hardware;
- analysis of information security methods;
- development of an application for a thesis.

The degree of analysis of the problem. When studying the topic of the thesis, domestic and foreign scientific works, textbooks, scientific articles in electronic publications were used.

When performing the work, computer technologies were used, in particular, the database was compiled in a Python environment, and the user interface was implemented through Django visual components. The work also uses the works and articles of domestic and foreign scientists.

Scope of the thesis: it is used to study the results obtained, as well as in society, for the work of small and medium-sized businesses.

МАЗМҰНЫ

КІРІСПЕ

Қазіргі уақытта біз қолданатын технологияларсыз қазіргі әлемді елестету қиын. Әрбір компания мен ұйым әртүрлі техникалық құрылғыларды пайдаланады, көптеген процестер автоматтандырылған, көптеген жүйелер жазбаша бағдарламалар бойынша жұмыс істейді, ал адам тек қызмет процесін бақылап, процестерді жеделдету үшін жаңа бағдарламалар жаза алады. Заманауи бағдарламалардың, сондай-ақ компьютерлік технологиялардың көмегімен адамдар қоғам өмірінің барлық салаларында үлкен биіктерге және өзгерістерге қол жеткізді. Алайда, оның осал жақтары бар, біріншіден, адам өз технологияларына тәуелді болды, екіншіден, енді бір технологияның осалдығы ұйымның толық осалдығына әкелуі мүмкін және оны өзімшілдік мақсатында қолдана алатындар бар. Әрине, жеке компьютердің қарапайым пайдаланушысы көп жағдайда тіпті өз компьютерін де қорғай алмайды, сондықтан ақпараттық қауіпсіздік сияқты мамандық пайда болды, оның басты мақсаты – ақпарат қауіпсіздігін қамтамасыз ету. Мысалы, қазір кез-келген ұйымның өз қауіпсіздік бөлімі бар, оның жұмысына ақпаратты қорғау кіреді.

Кәсіпорындағы ақпаратты кешенді қорғауды зерттеудің өзектілігі стандартты режимде жұмыс істейтін автоматтандырылған жүйені рұқсатсыз басқару әсерлерінен және үшінші тұлғалардың ұрлау немесе тұтастығын бұзу мақсатында айналымдағы ақпаратқа қол жетімділігін шектеу қажеттілігімен байланысты.

Кәсіпорындағы ақпаратты кешенді қорғау деп ақпаратты қасақана немесе кездейсоқ рұқсатсыз кіруден, сондай-ақ деректерді ұрлаудан, өзгертуден және жоюдан қорғау техникасын түсіну керек.

Ақпаратты кешенді қорғау мәселесі қызметкерлердің қызметімен, бағдарламалық-техникалық тораптар мен агрегаттардың сапасымен және сенімділігімен байланысты, бұл ақпаратты қорғау жөніндегі табысты және тиімді іс-шараларды іске асыру кезінде зиянды әсерлерді іске асыру ықтималдығын арттыруға әкеп соғады.

Дипломдық жұмыстың мақсаты – компанияның ақпараттық қауіпсіздігінің кешенді жүйесін жобалау.

Қойылған мақсатқа жету үшін жұмыста келесі міндеттер орындалуы керек:

- ақпараттық қауіпсіздік түсінігіне теориялық зерттеулер жүргізу;
- оның кәсіпорында саласында қолдану ерекшеліктері анықтау;
- бағдарламалық-аппараттық құралдарына сипаттама жасау;
- ақпаратты қорғау әдістерін талдау;
- диплом жұмысы бойынша жүйе әзірлеу.

Зерттеу объектісі. Python тілінде жазылған кешенді жүйе.

Мәселені талдау дәрежесі. Дипломдық жұмыстың тақырыбын зерттеу барысында отандық және шетелдік ғылыми еңбектері мен оқулықтар, электронды басылымдардағы ғылыми мақалалар қолданылды.

1 Пәндік саланы теориялық талдау

1.1 Ақпараттық қауіпсіздік түсінігі

Ақпараттық қауіпсіздік (АҚ) – ақпаратты жинау, өңдеу, сақтау, іздеу, беру және қабылдау кезінде ақпараттың бүлінуін, бұрмалануын және жария етілуін болдырмаудың әкімшілік және техникалық әдістеріне жатады. Жеткізуші тарапынан бұл ішкі және сыртқы қауіп факторларынан аппараттық құрал, мәліметтер базасы, желілер мен жүйелер сияқты байланыс және компьютерлік құралдар сияқты ақпараттық активтерді қауіпсіз қорғау және пайдалану бойынша бірқатар іс-шаралар, ал пайдаланушы тарапынан жеке ақпараттың ағып кетуіне және теріс пайдаланылуына жол бермеу қажет [1].

Ақпараттық қауіпсіздік ұғымы ақпаратты және деректердің әртүрлі түрлерін заңсыз зерттеуден, пайдаланудан, жоюдан қорғау ретінде анықталады. Сондай-ақ, ақпараттық қауіпсіздік ақпаратты рұқсатсыз таратуға әкелетін әрекеттерден қорғауды қамтиды. Нашар қорғалған деректерге әсер ету әр түрлі болуы мүмкін.

Оларға:

- алаяқтардың шабуылы;
- қызметкерлер жіберетін қателіктер;
- аппараттар мен бағдарламалық техниканың жұмысын тоқтату;
- табиғи апаттар, мысалы, дауыл, өрт немесе жер сілкінісі [2].

Егер деректердің құпиялылығына, тұтастығына және сенімділігін сақтауға кепілдік беретін іс-шаралар жүзеге асырылса, ақпараттық қауіпсіздікке қол жеткізуге болады. Деректерді қорғау ақпаратқа жедел қол жеткізуді қамтамасыз етуге арналған. Ақпараттық қауіпсіздік ықтимал қауіптерді қамтамасыз етуі және сақталатын немесе берілетін ақпараттың заңды маңыздылығын растауы керек. Қажет болған жағдайда ақпарат пен оның ресурстарына тиісті қол жетімділік ашық болуы керек. Бұл деректердің негізгі қасиеттері, онсыз олардың тиімділігі күрт төмендейді [3].

Қауіп тұтас деректер жүйесінде осал, әлсіз жақтардың болуын көрсетеді. Егер бағдарламашы бағдарламаларды жасаған кезде байқаусызда дәлсіздік жасаса, осалдықтар пайда болуы мүмкін.

Кейбір қауіптер басқаларынан ерекшеленетін параметрлер:

- жоюға арналған ақпаратқа жататын қасиеттер;
- ақпараттық жүйенің элементтері – оларға компьютерлік жүйені қолдау үшін мәліметтер, бағдарламалық жасақтама, жабдық, инфрақұрылым кіреді;
- қауіп-қатердің нұсқасы – күтпеген немесе қасақана қате, табиғи апаттар пайда болады;
- қауіптілік көзінің орналасқан жері – ақпараттық жүйенің ішінде немесе одан тыс [4].

Ақпаратты қорғаудың көптеген нюанстарын ескеретін әдіс әртүрлі стандарттарда көрінеді. Оның негізін ақпараттық қауіпсіздіктің ішкі саясатын

әзірлеу құрайды. Ол қауіптің көздерін анықтауға арналған. Ол үшін ең алдымен құпия ақпаратты сақтау үшін бар техникалық құралдар қолданылады [5].

Қауіпсіз ақпарат бірнеше деңгейде жүзеге асырылады:

− егер сөз ақпаратты заңнамалық қорғау туралы болса, тиісті ұғымдар, талаптар мен ережелер заңнамалық және нормативтік актілерде, халықаралық үлгідегі ресми қағаздарда көрсетіледі;

− әкімшілік деңгей – кәсіпорын басшылығы бекітетін іс-шаралар;

− процедураға сәйкестік – бұған адамдар жүзеге асыратын ақпаратты қорғау шаралары кіреді;

− бағдарламалар мен техникалық құралдарды қолданысқа енгізу – практикалық іс-шаралар [6].

Кәсіпорында ақпараттық қауіпсіздікті құрудың негізгі міндеті – деректерді қорғау, атап айтқанда ұйымға зиян келтірместен олардың тұтастығы мен қол жетімділігін қамтамасыз ету.

Бүгінгі таңда ақпараттық қауіпсіздіктің жоғары деңгейіне қол жеткізуге көмектесетін бірнеше әдістер мен техникалық құралдар бар.

Кәсіпорынның ақпаратты қорғаудың өзіндік жүйесін анықтау мақсаттарды нақты қоюдан, құнды корпоративтік ақпаратты сақтауға бағытталған нақты қадамдарды жоспарлаудан басталады. Процестің барлық қатысушыларының қауіпсіздік саясатын сақтауы, ақпараттық қауіпсіздіктің жаңа әдістерін енгізу ұйым қызметінің әртүрлі салаларына толық әсер етуге мүмкіндік береді. Негізгі бағыт – жүз пайыз қауіпсіздік және аутентификацияны, құпиялылықты, тұтастықты бұзудан қорғау жағдайларын жасау [7].

Кәсіпорынның ақпаратты қорғау саясатының орындалуын бақылау мәселесіндегі негізгі жүктеме қауіпсіздік қызметіне жүктеледі. Қызметкерлердің ақпаратпен дұрыс жұмыс істеуі алға қойылған мақсаттарға тікелей байланысты. Мысалы, қызметкерге белгілі бір қағаздарға қол жеткізуді ұсынған кезде, бұлтты сақтау арқылы деректерді беруге назар аударған жөн – оны қорғау керек; криптографиялық қорғауды пайдалану құжаттарды рұқсатсыз жүктеу мүмкіндігін барынша шектейді.

Ақпаратты пайдалануға қол жеткізу деңгейлерін ажырату сұраныстарды үйлестіруге, қызметкерлер арасындағы функцияларды бөлуге, рұқсат етілген және тыйым салынған әрекеттерді уақтылы анықтауға көмектеседі. Бұл өңделген ақпаратпен дұрыс емес, заңсыз әрекеттерді тоқтатып қана қоймай, осы мәліметтермен жұмыс кезінде ауытқулар анықталған кезде ақпаратпен жұмысты түзетуге көмектеседі [8-9].

АҚ қағидаттарын егжей-тегжейлі қарастырайын:

1) Ақпараттық жүйені(АЖ) - пайдаланудың қарапайымдылығы. Ақпараттық қауіпсіздіктің бұл қағидасы қателерді азайту үшін ақпараттық жүйені пайдаланудың қарапайымдылығын қамтамасыз ету болып табылады. АЖ-ны пайдалану кезінде пайдаланушылар мен әкімшілер абайсызда қателіктер жібереді, олардың кейбіреулері қауіпсіздік саясатының талаптарын орындамауға және ақпараттық қауіпсіздік деңгейін төмендетуге әкелуі мүмкін.

Пайдаланушылар мен әкімшілердің операциялары неғұрлым күрделі, шатастыратын және түсініксіз болса, соғұрлым олар қателіктер жібереді. АЖ-ны пайдаланудың қарапайымдылығы қате әрекеттердің санын азайтудың қажетті шарты болып табылады. Ақпараттық қауіпсіздіктің бұл қағидаты архитектураның қарапайымдылығын және АЖ функционалдығын төмендетуді білдірмейді.

2) Барлық операцияларды бақылау. Бұл принцип ақпараттық қауіпсіздік жағдайын және АҚ-ға әсер ететін барлық оқиғаларды үздіксіз бақылауды білдіреді. Қажетсіз әрекеттерді блоктау және ақпараттық жүйенің қалыпты параметрлерін тез қалпына келтіру мүмкіндігімен кез-келген IP объектісіне кіруді бақылау қажет.

3) Рұқсат етілмегеннің бәріне тыйым салынған. АҚ-ның бұл қағидасы, мысалы, бизнес-процестің регламентінде немесе қорғаныс бағдарламалық жасақтамасының параметрлерінде көрсетілген тиісті ереже болған кезде ғана АЖ-ның кез-келген объектісіне қол жеткізу керек. Бұл жағдайда АҚ жүйесінің негізгі функциясы кез-келген әрекетке тыйым салу емес, шешім болып табылады. Бұл принцип тек белгілі қауіпсіз әрекеттерге жол береді және кез-келген қауіпті тануға жол бермейді, бұл көп ресурстарды қажет етеді, АҚ-ның толық емес және жеткілікті деңгейін қамтамасыз етпейді.

4) Ашық IP архитектурасы. Ақпараттық қауіпсіздіктің бұл қағидасы қауіпсіздік түсініксіздік арқылы қамтамасыз етілмеуі керек. Ақпараттық жүйені компьютерлік қауіп-қатерлерден IP-нің әлсіз жақтарын қиындату, шатастыру және жасыру арқылы қорғауға тырысу, сайып келгенде, мүмкін емес және сәтті хакерлік, вирустық немесе инсайдерлік шабуылды кешіктіреді.

5) Қол жеткізуді ажырату. АҚ-ның осы қағидаты әрбір пайдаланушыға оның өкілеттіктеріне сәйкес ақпаратқа және оның тасымалдаушыларына қолжетімділік беріледі. Бұл ретте өкілеттіктерді асыра пайдалану мүмкіндігі алынып тасталды. Әр рөлге/лауазымға/пайдаланушылар тобына белгілі бір IP объектілеріне әрекеттерді орындау (оқу/өзгерту/жою) құқығын тағайындауға болады.

6) Минималды артықшылықтар. Минималды артықшылықтар принципі – пайдаланушыға ең аз құқықтар беру және бағдарламалардың қажетті функционалдығын барынша азайту. Мұндай шектеулер жұмысты орындауға кедергі келтірмеуі керек.

7) Жеткілікті төзімділік. Ақпараттық қауіпсіздіктің бұл қағидасы ықтимал шабуылдаушылар жеткілікті күрделі есептеу тапсырмалары түрінде кедергілерге тап болуы керек екендігінде көрінеді. Мысалы, кіру паролін бұзу хакерлерден үлкен уақыт аралықтарын және/немесе есептеу қуатын талап етуі керек.

8) Бірдей процедуралардың минимумы. Ақпараттық қауіпсіздіктің бұл қағидасы АҚ жүйесінде бірдей парольді енгізу сияқты бірнеше пайдаланушыларға ортақ рәсімдер болмауы керек. Бұл жағдайда ықтимал хакерлік шабуылдың ауқымы аз болады [10].

1.2 Кәсіпорынның ақпараттық қауіпсіздігі

Қазіргі әлемнің киберқауіптеріне жақсы бағдарланған компания тәуекелдер деңгейіне сәйкес ақпараттық қауіпсіздік жүйесін құру қажеттілігін сезінеді. Бірақ қабылданған шешімдер қымбат болмауы керек және сонымен бірге тиімді болып қалуы керек. Ақпараттық қауіпсіздік стратегиясын құру кезінде бизнестің нақты қажеттіліктеріне назар аудару қажет [11].

Кез-келген жүйе, оның ішінде кәсіпорындағы ақпараттық қауіпсіздік жүйесі оны құратын және оның ережелеріне сәйкес әрекет ететін адамдардан басталады. Сондықтан бірінші кезең сипаттау қажет стратегияны әзірлеу болады:

− болжанатын тәуекелдер, олардың түрі қорғалатын ақпараттың құпиялылық дәрежесіне және компанияның дербес деректер операторы болып табылатындығына байланысты. Екінші жағдайда стратегияның негізгі ережелері реттеушілердің ұсыныстарына негізделеді;

− ақпараттық қауіпсіздік архитектурасынан күтулер, орнатуға жоспарланған бағдарламалық және аппараттық құралдар;

− жүйені әзірлеуге және енгізуге жұмсалатын қаржы ресурстары;

− стратегияны іске асыруға қатысатын персонал-меншікті, тартылған сарапшылар, аутсорсингтегі компания;

− енгізудің жоспарланған мерзімдері [12].

Стратегия бекітілгеннен кейін ұйымдастырушылық және әкімшілік құжаттар пакетін әзірлеу және енгізу қажет.

Минималды нұсқада үш құжатты әзірлеу және қабылдау қажет:

1 Ақпараттық қауіпсіздік саясаты.

2 Ақпараттық қауіпсіздік тұжырымдамасы.

3 Коммерциялық құпия туралы ереже (құпия ақпарат).

Бұдан басқа, қолданбалы сипаттағы әдістемелік нұсқаулықтарды әзірлеу қажет [13].

Ақпараттық қауіпсіздік саясаты

Құжат ұйым үшін негіз болып табылады, егер мүмкін болса, оны Компанияның атқарушы басшылығы деңгейінде емес, Директорлар кеңесі деңгейінде бекіту керек, өйткені онда сипатталған ережелер жоғары менеджменттің мінез-құлқын реттейді.

Құжатта келесі деректер сипатталған:

− құжаттардың құпиялылық деңгейлері;

− ақпаратпен және оның тасымалдаушыларымен жұмыс істеудің негізгі регламенттері;

− пайдаланушыларды қабылдау ережелері;

− ақпараттық қауіпсіздік қатерлері мен тәуекелдері.

Ақпараттық қауіп-қатерлер деңгейі үнемі өзгеріп отыратындықтан, ақпараттық қауіпсіздік саясатын жыл сайын қайта қарау орынды.

Ақпараттық қауіпсіздік тұжырымдамасы

Клиенттің деректерімен жұмыс істейтін компания үшін іскерлік беделді сақтау және ақпараттың құпиялылығын сақтау үшін барлық шараларды қолданатындығын растау маңызды. Ол үшін стратегия мен саясаттан шағын сығуды дайындау керек, онда ақпаратты қорғаудың негізгі шаралары мен құралдары көрсетілген. Бұл құжатты компанияның веб-сайтына клиенттер үшін ашық қол жетімділікте орналастыру ұйымның жағымды имиджін жасайды.

Коммерциялық құпия туралы ереже

Әрбір кәсіпорында құпия ақпараттың белгілі бір көлемі қалыптасады, бірақ ол барлық жерде коммерциялық құпияға жатпайды, оның жариялануы заңмен қудаланады. Бұл үшін компания коммерциялық құпия режимін жариялап, құпия ақпаратпен жұмыс істеудің негізгі ережелерін реттейтін ереже шығаруы керек.

Ережеде:

1) Ақпаратты коммерциялық құпияға жатқызу тәртібі;
2) Коммерциялық құпиясы бар құжаттармен және файлдармен жұмыс істеу тәртібі;
3) Коммерциялық құпия режимін сақтауға жауапты тұлғалар мен бөлімшелер;
4) Құпия деректерді жария еткені үшін тәртіптік немесе персоналды демотивациялауға байланысты жауапкершілік шаралары.

Барлық қызметкерлер осы құжатпен таныстырылуы керек, сонымен бірге еңбек шарттарына құпиялылықты сақтау үшін жауапкершілік туралы ереже енгізілуі керек. Бұл жағдайда ақпарат қасақана ағып кетсе, кінәлі адамнан залалды азаматтық-құқықтық тәртіпте өндіріп алуға болады, ал заңмен қорғалатын мүдделерге айтарлықтай зиян келтірілген жағдайда бұл адамды қылмыстық жауапкершілікке тартуға болады. Мұндай алдын-алу шаралары кейде құжаттар мен файлдарды рұқсатсыз кіруден физикалық және бағдарламалық қорғау шараларына қарағанда құпия ақпаратты жоғалту немесе ауыстыру қаупінен жақсы қорғайды.

Қызметкерлердің мінез-құлқын реттейтін және жауапкершілік шараларын енгізетін құжаттар ұйым қызметкерлеріне, инсайдерлерге әсер етуі мүмкін, олар статистикаға сәйкес ақпараттың 80% - ға жуық ағып кетуіне жауап береді, бірақ 20% сыртқы себептерге байланысты. Аудит қауіпсіздік жүйесіндегі осалдықтарды табуға көмектеседі, оны өз бетінше немесе тартылған мамандардың көмегімен ұйымдастыруға болады. Осалдық сканерлері аудит кезінде орын алған барлық қатерлерді ескере отырып, хакерлердің іс-әрекеттерін имитациялайды және кәсіпорындағы ақпараттық қауіпсіздік жүйесінде әлсіз жерлерді табады. Осы мәліметтер негізінде құпия ақпаратты қорғаудың бағдарламалық және техникалық шаралары бойынша ұсыныстар жасауға болады. Аудит көлемі желінің архитектурасына, таралу дәрежесіне, бұлтты технологияларды пайдалануға байланысты [14].

Кәсіпорындағы ақпараттық қауіпсіздік жүйесі аутсорсингтік компанияларды шақыру немесе біреудің сәтті тәжірибесін зерттеу арқылы

әртүрлі тәсілдермен ұйымдастырылған. Ақпараттық қауіпсіздік мысалдары бизнестің әртүрлі салаларында мәселенің қалай шешілетінін көрсетеді.

Қазақстандық банктер мен компанияларда ақпараттық қауіпсіздік жүйесінің қалай енгізілгенін көрсететін бірқатар жағдайларды талдау қызықты.

Мәселе екі жолдың бірімен шешіледі:

- өз күшімен;
- мердігерлерді тарта отырып [15].

Қазақстанда киберқауіптермен күресуге мамандандырылған компаниялардан жетекші киберқауіпсіздік мамандарын мердігерлермен жұмыс істеу кезінде күтілетін деректердің ағып кету қаупін болдырмай, АҚ-ның жеке моделін құру мақсатында ірі ресейлік корпорацияларға тарту үрдісі байқалады. Банктер Ресей Федерациясының Орталық банкіне аутсорсерлермен жұмыс істеу ережелеріне сәйкес арнайы стандарт шығару арқылы ақпараттық қауіпсіздіктің осындай тәуекелдерінің болуы туралы ескертеді, олар кәсіпорын үшін де өзекті болады.

Ақпараттық қауіпсіздікті қорғау үшін бағдарламалық жасақтаманы таңдау тұрғысынан ұлттық өндірушіні қолдаудың мемлекеттік саясаты мемлекеттік қатысуы бар немесе мемлекеттік келісімшарттармен белсенді жұмыс істейтін ресейлік корпорацияларды ресейлік Бағдарламалық жасақтамаға ауысуға шақырады. Шағын бизнес оны бағаға қол жеткізу, жоғары сенімділік, АЖ-ның тар секторларында ақпараттық қауіпсіздікті қамтамасыз ету себептері бойынша артық көреді. Импортты алмастыру саясатының кемшілігі-бірыңғай ресейлік операциялық жүйенің болмауы. Қолданыстағы 20-дан астам өнім стратегиялық міндеттерді емес, тактикалық мәселелерді шешеді және компаниялар Windows және Linux-тағы осалдықтарға төтеп беруге мәжбүр. WannaCry вирусының эпидемиясы, бүкіл әлемдегі зауыттар мен ауруханаларды тоқтатқан және ондаған миллиард долларға бағаланған залал келтірген шифрлаушы олардың кибер алаяқтарға жақсы таныс екенін дәлелдейді [16].

Қауіп моделін құру

АҚ жүйесін таңдау тәуекелдер деңгейіне байланысты. Қауіп-қатер моделі көбінесе бизнеске негізделген. Сонымен, ақпараттың ағуы телекоммуникациялық компанияларға, бағдарламалық жасақтаманы жасаушыларға, медицинаға тән. Банктер үшін клиенттердің шоттарынан рұқсатсыз ақша аудару әрекеттері қауіпті. Даркнетте тек банктер мен ұялы байланыс операторларының ғана емес, сонымен қатар оқу орындарының да мәліметтер базасы пайда бола бастады.

Жаңа вирустар әскери құрылымдардың қатысуымен жасалады. WannaCry-де олар американдық әскери бөлім хакерлер тобына берілген негізгі шешімдерді көрді. Ирандық Stuxnet, сонымен қатар өнеркәсіптік кәсіпорындарды нысанаға алып, мыңдаған өндірістерді тоқтатты, Израиль барлауымен құрылды. Ақпараттық қауіпсіздіктің жоғары дәрежесін қамтамасыз етпейтін жалпы пайдаланушылық операциялық жүйелерді пайдаланатын орта кәсіпорын кез-келген уақытта жекелеген елдерге немесе экономика салаларына

әсер ететін жаңа вирустың құрбаны болуы мүмкін деп болжауға болады. Ernst & Young компаниясы жүргізген әлемнің ірі кәсіпорындарының 200 бас директорларының сауалнамасына сәйкес, таяудағы бес-он жылда киберқауіптер әлемдік экономика үшін ақпараттық қауіпсіздік қатерлері арасында бірінші орынға шығады.

Бұл қорғаныс жүйелерін әзірлеу кезінде сіз кәсіпорынның ақпараттық қауіпсіздігінің енгізілген мысалдарына толығымен сенбеуіңіз керек, негізгі кезеңде барлық осалдықтарды тексеріп, болжанған әлсіздіктерді жою қажет. Негізгі проблема 1970 жылдары Ресей Федерациясының көптеген кәсіпорындарында құрылған ақпараттық жүйелердің архитектурасы болып табылады және күрделілік өскен сайын қауіпсіздіктің жалпы мәселелерін шешпейді, бірақ осалдықтарды уақытша және оңай бұзылатын шешімдермен жабады. Көптеген АЖ нашар қорғалған, оларды зиянды бағдарламамен жұқтыру немесе бұзу қиын емес. Жеке қорғаныс жүйесін құру кезінде бұзу құны теориялық пайданың құнынан жоғары болуы керек қағидасына сүйену керек, нарық сарапшылары өз шешімдерін алға жылжытуды талап етеді.

2019 жылы компаниялар мен азаматтарға бағытталған 231 хакерлік науқан тіркелді. Пайдаланылған шабуыл құралдарының ішінде көшбасшылар зиянды бағдарламалар мен әлеуметтік инженерия әдістері болды, 2018 жылы мұндай науқандар 217 болды және олар негізінен парольдер мен сәйкестендіру құралдарын жинауға бағытталған. Бірақ көптеген кәсіпорындар мен бұлтты қызметтер ақпараттық қауіпсіздіктің жоғары деңгейін қамтамасыз ететін аутентификацияның екі факторлы моделіне көшкеннен кейін қауіп-қатердің бағыты өзгерді [17].

1.3 Ақпараттық қауіпсіздікті қамтамасыз ету жүйесінің бағдарламалық-аппараттық құралдары

Ақпарат әр түрлі компаниялар, фирмалар, кез-келген коммерциялық және мемлекеттік құрылымдар үшін, олардың қызмет саласына қарамастан құнды ресурс болып табылады. Осыған байланысты мұндай нысандар Киберқауіпсіздіктің толыққанды және тиімді жүйесін құруға мүдделі. Оны ұйымдастыру ақпараттық қауіпсіздікті қамтамасыз етудің мамандандырылған және ең қолайлы құралдарын қолдануды талап етеді. Киберқауіпсіздік жүйесінің негізгі мақсаты – ақпараттық жүйені қорғау, сақталуы, қорғалатын деректердің тұтас, өзгертілмейтініне, жойылмайтынына кепілдік жасау. Киберқауіпсіздікті қамтамасыз ету процестері әртүрлі қорғау тетіктерін қолдана отырып іске асырылады, оларды қалыптастыру кезінде мынадай құралдар пайдаланылуы мүмкін: физикалық, аппараттық, бағдарламалық, бағдарламалық-аппараттық(техникалық),криптографиялық, ұйымдастырушылық, құқықтық, моральдық-этикалық [18].

Физикалық. Ақпараттық қауіпсіздікті қамтамасыз етудің физикалық құралдары электронды, механикалық жабдық түрінде ұсынылған, ол ену

жолдарында физикалық кедергілерді қалыптастыруға және жүйенің немесе ақпараттың белгілі бір компоненттеріне бұзушыларға рұқсатсыз қол жеткізуге арналған.

Аппараттық. Киберқауіпсіздік жабдықтары – бұл автоматтандырылған ақпараттық жүйенің жабдықтарына біріктірілген немесе осы жабдықпен біріктірілген автономды жабдық ретінде жұмыс істейтін электронды, механикалық құрылғылардың барлық түрлерін ұсынатын кең санат. Аппараттық құралдардың негізгі міндеті құрылымдық элементтерді, компьютерлік жүйелерді (мысалы, орталық процессорлар, перифериялық құрылғылар, терминалдар және т.б.) ішкі қорғауды қамтамасыз ету болып табылады.

Ақпараттық. Ақпараттық қауіпсіздікті қамтамасыз етудің бағдарламалық құралдары логикалық және зияткерлік қорғау функцияларын іске асыру үшін қолданылады. Бағдарламалық жасақтама қорғаудың ең танымал, кеңінен қолданылатын түрлерінің бірі болып табылады, өйткені олар әмбебаптығымен, пайдаланудың қарапайымдылығымен, оларды өзгерту және дамыту мүмкіндіктерінің болуымен ерекшеленеді.

Апаратты-ақпараттық. Киберқауіпсіздікті қамтамасыз етудің аппараттық-бағдарламалық құралдары – бұл ұйымның автоматты жүйесінің құрылымына кіретін және дербес немесе өзге құралдармен біріктіріп қорғау функционалын орындайтын электрондық құрылғылардың, гаджеттердің, мамандандырылған БҚ-ның әртүрлі түрлері.

Криптографиялық. Ақпараттық қауіпсіздікті қамтамасыз етудің криптографиялық құралдары аппараттық және/немесе бағдарламалық құралдарды пайдалана отырып іске асырылуы мүмкін. Деректерді қорғаудың криптографиялық әдістері оларды шифрлау принципіне негізделген.

Әкімшілік. Киберқауіпсіздікті қамтамасыз етудің әкімшілік (ұйымдастырушылық) құралдары ақпаратты өңдеу жүйесінің жұмыс рәсімдерін, ақпараттық жүйенің ресурстарын пайдалану процестерін, ұйым қызметкерлерінің кәсіби қызметін, компания қызметкерлерінің ақпараттық жүйемен өзара іс-қимыл тәртібін өзекті киберқауіптерді іске асыру ықтималдығын барынша қиындататындай немесе мүлдем болдырмайтындай не киберқауіптерді іске асыру жағдайында ысыраптардың мөлшерін барынша азайтатындай етіп регламенттейді.

Құқықтық. Киберқауіпсіздікті қамтамасыз етудің құқықтық құралдары - қолданыстағы федералды заңнама, президенттік жарлықтар, нормативтік құжаттар, салалық реттеушілердің талаптары мен техникалық регламенттері. Барлық осы ресми құжаттаманың көмегімен ақпараттық деректермен өзара әрекеттесу ережелері реттеледі, деректерді өңдеу, пайдалану кезінде ақпараттық қатынастарға қатысушылардың құқықтары мен міндеттері бекітіледі, сондай-ақ саладағы заңнаманы бұзғаны үшін әкімшілік немесе қылмыстық жауапкершілік белгіленеді.

Моральды-этикалық. Киберқауіпсіздікті қамтамасыз етудің моральдық-этикалық құралдары ақпаратпен (оның ішінде құпия ақпаратпен) өзара іс-

қимылдың жалпы қабылданған және/немесе нақты ұйымда іске асырылатын мінез-құлық нормалары мен регламенттері түрінде ұсынылған. Электрондық есептеу жабдықтарын тарату процесінде моральдық-этикалық нормалар дәстүрлі түрде қалыптасады (кейбіреулері бұрыннан қалыптасқан) [19-20].

2 Ақпараттық жүйені жобалау

2.1 Функционалдық-құрылымдық сұлба

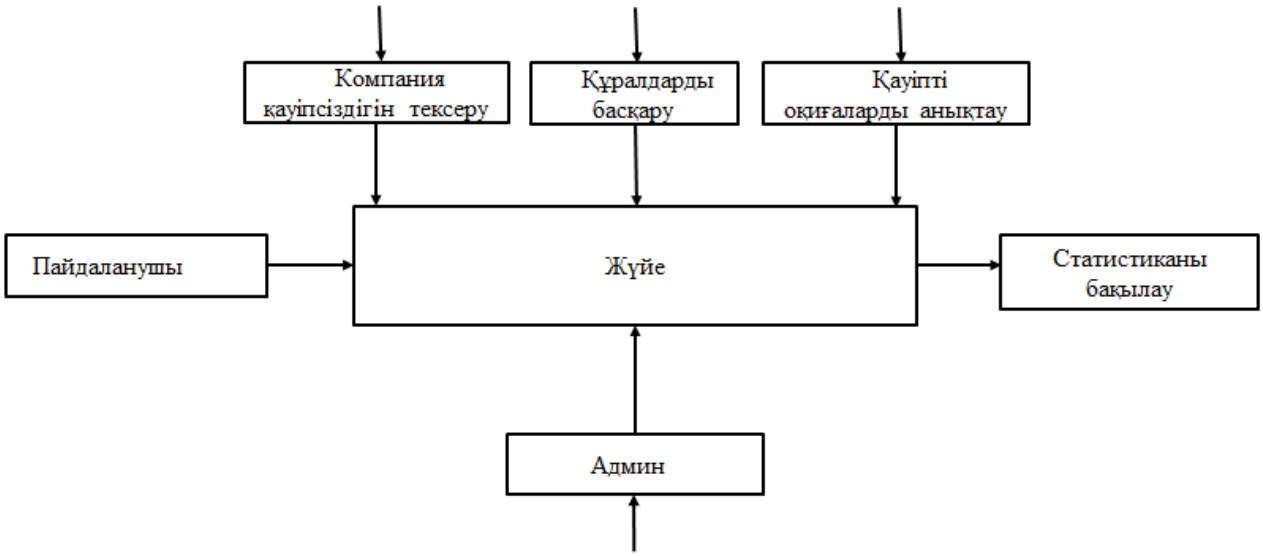
Функционалдық құрылымдық сұлба – жүйелік инженерия мен бағдарламалық жасақтаманы жасаудағы функционалды блок-схема. Ол жүйенің функциялары мен қатынастарын сипаттайды.

Функционалды блок-схема:

- блоктармен бейнеленген жүйенің функциялары
- сызықтармен бейнеленген блоктың кіріс және шығыс элементтері,
- функциялар арасындағы қатынастар,
- сондай-ақ, материя және/немесе сигналдар үшін функционалды тізбектер мен жолдар

Блок-схема белгілі бір қасиеттерді көрсету үшін қосымша схема таңбаларын қолдана алады.

2.1-суретте компания қауіпсіздігінің кешенді жүйесі жұмысының құрылымдық сұлбасы көрсетілген.



2.1-сурет – Функционалдық диаграмма

2.2 Прецеденттер диаграммасы

Прецеденттер диаграммасы – бұл жоба жоспарындағы әрекеттерді жоспарлау құралы. Бұл жоба кестесінің желілік диаграммасын құру әдісі, ол әрекеттерді көрсету үшін түйіндер деп аталатын блоктарды қолданады және оларды тәуелділіктерді көрсететін көрсеткілермен байланыстырады.

Негізгі элементтерге прекурсорларды анықтау және келесі атрибуттарды анықтау кіреді:

- ерте басталу күні;

– кеш басталу күні;
– ерте аяқталу күні;
– кеш аяқтау;
– ұзақтығы;
– қызмет атауы;
– WBS сілтемесі.

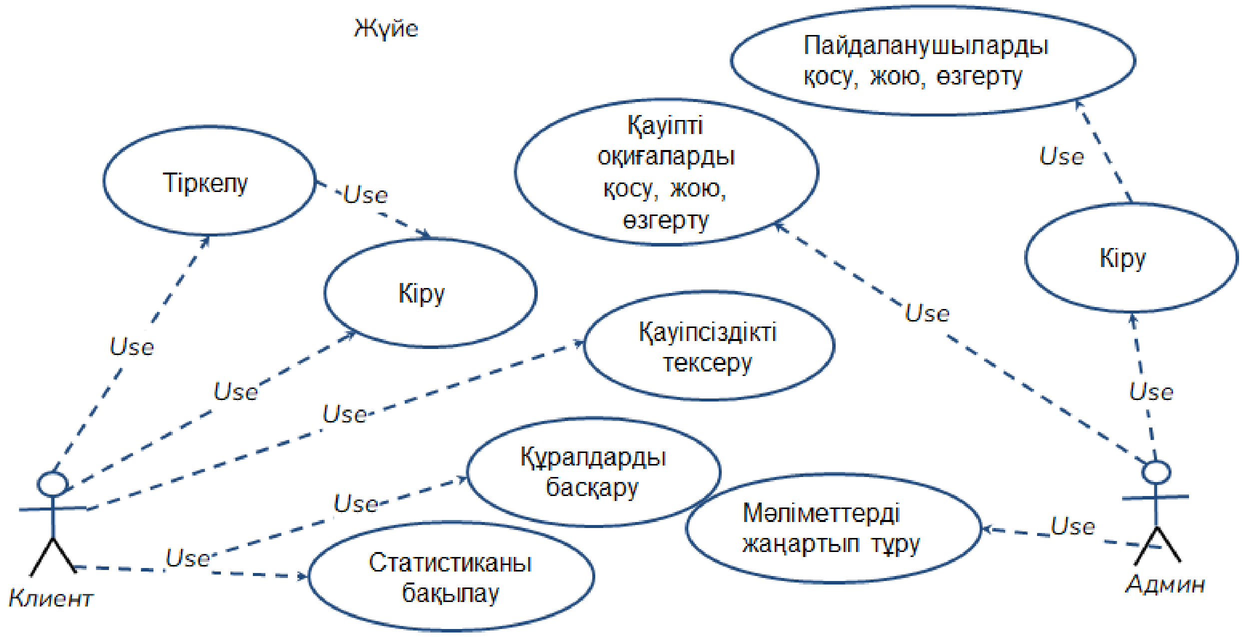
Жүйеде 2 қолданушы бар: админ және клиент.

Әрқайсысының өзіндік мүмкіндіктері бар:

Клиент – компания қауіпсіздігін тексере алады және ақпараттар бойынша статистикаға қол жеткізе алады.

Админ – мәліметтерді жаңарта алады, қауіптердің күйін енгізеді, пайдаланушыларды қосу/жою/өзгертуге мүмкіндігі бар.

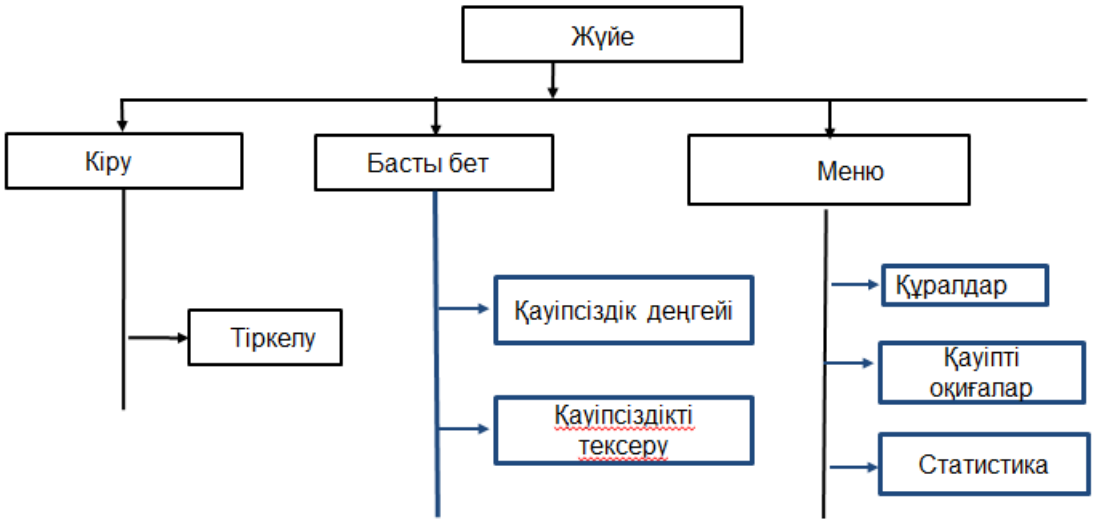
Екеуінде де программаға тіркелу мүмкіндігі бар. Мысалын төмендегі 2.2-суретте көре аламыз:



2.2 - сурет – Жүйенің прецедenttер диаграммасы

2.3 Навигациялық сұлба

Навигация схемасы әдетте мәзірлер мен ішкі мәзірлер жиынтығы, сонымен қатар қосымша сайт картасы ретінде ұсынылады, дегенмен бұл веб-сайттарда бұрынғыға қарағанда аз таралған. Веб-сайтты, интернетті немесе порталды шарлау схемасы адамдарды іздеу, есептер, оқиғалар, кеңселердің орналасуы, қаржылық деректер және т.б. сияқты әртүрлі жалпы тапсырмалар түрлерімен әр түрлі пайдаланушылар топтарына қызмет ету үшін жасалған мазмұн құрылымын көрсетеді. Мысалын төмендегі 2.3-суретте көре аламыз:



2.3 - сурет – Навигация сызбасы

3 Бағдарламалық қамтамасын құру

3.1 Қолданылатын бағдарламалау орталары

Дипломдық жұмысты орындау барысында компания қауіпсіздігінің кешенді жүйесі әзірленді. Ол үшін Python және оның scapy, nmap кітапханалары, Django, HTML, CSS, JavaScript бағдарламалау құралдары қолданылды.

3.1.1 Python

Python – алғашында Гвидо ван Россумның «Амеба» бөлінген операциялық жүйесін жүйелік басқаруға арнап жасақтаған бағдарламалау тілі болып табылады. Жаңа версияларының шығуына байланысты әр версияда түрлі функциялар қосылып отырады, дәл қазіргі уақытта соңғы нұсқасы – 3.10.4. Қазіргі уақытта Python-ды көптеген бастаушы және кәсіби бағдарлама жасақтаушылар тек машиналық оқытуда ғана емес, веб-қосымшаларды әзірлеуде де қолданады [21].

Python-да оны көптеген басқа тілдерден жоғары икемділік пен динамизммен ерекшелейтін бірнеше мүмкіндіктер бар.

Мысалы, сынып объект болып табылады, ал ата-ана сыныптарының тізіміндегі сыныпты анықтау мәлімдемесінде өрнектерді қолдануға болады.

Естилмейд ватсап без звука

```
def get_class():
   return dict
class D(get_class()):
   pass
d = D()
```

Орындау кезінде көптеген нысандарды өзгертуге болады, мысалы, сыныптар:

```
>>> class X(object): pass
…
>>> y = X()
>>> y.wrong_method()  # бұл әдіс әлі жоқ
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
AttributeError: 'X' object has no attribute 'wrong_method'
>>> X.wrong_method = lambda self : 'im here' # қосамыз
>>> y.wrong_method() # себебі әдіске қол жеткізу  _dict_ класса бағдарламалық іздеуге әкеледі,
'im here' # то wrong_method барлық даналарға қолжетімді болады
```

Функция декораторлары – басқа функцияны дәлел ретінде қабылдайтын шақырылған объектілер. Функция декораторлары функциямен жұмыс жасай алады және функцияның өзін немесе оны алмастыратын басқа функцияны немесе шақырылған нысанды қайтара алады. Яғни, егер декорат деп аталатын декор бұрын кодта жазылған болса, онда келесі код:

```
@decorate
def target():
   print('running target()')
```

осыған тең:

```
def target():
   print(running target())
   target = decorate(target)
```

Функция декораторын қолдану мысалы:

```
>>> def deco(func):
...     def inner():
...         print('running inner()')
...     return inner
…
>>> @deco
... def target():
...     print('running target()')
>>> target()
running inner()
>>> target
<function deco.<locals>.inner at 0.10063b598>
```

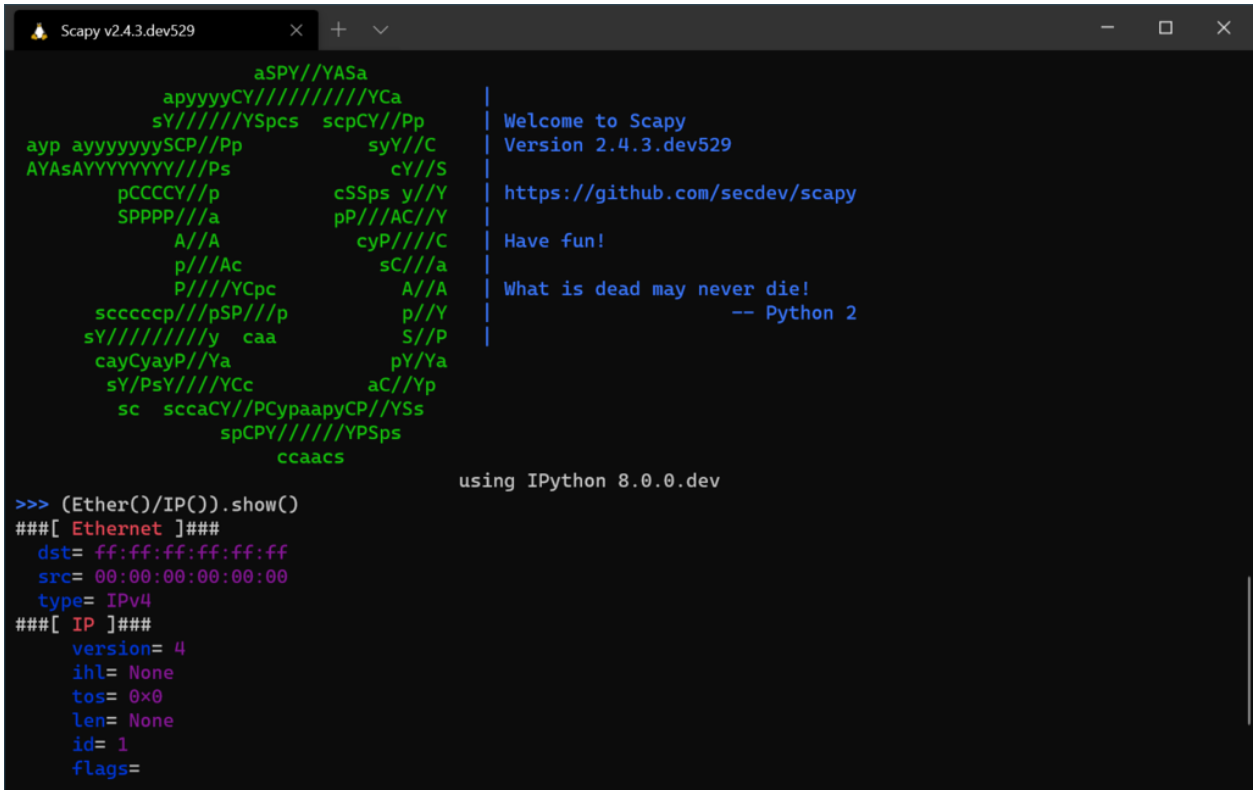
3.1.1.1 Scapy

Scapy – Python бағдарламалау тілінде желілік пакеттерді басқаруға арналған интерактивті қабық және бағдарламалық кітапхана. Scapy 2003 жылы Филипп Бионди жазған және GPLv2 лицензиясы бойынша таратылады [22].

Scapy libpcap кітапханасын пайдаланады және оны желілік трафикті ұстап алу және талдау үшін де, пакет құрастырушысы ретінде де пайдалануға болады. Сонымен қатар стандартты протоколдарды қолдану, Scapy-де пакеттерді талдау және құру кезінде өздерін құруға және пайдалануға мүмкіндік бар.

Scapy-дің ерекшелігі – кодтың бірнеше жолында әртүрлі тапсырмаларға бейімделу мүмкіндігі.

Scapy желілік интерфейстерге қол жеткізуді қажет ететіндіктен, оны супер пайдаланушының артықшылықтарымен іске қосу керек болады [23].



3.1-сурет – Scapy 2.4.3

3.1.1.2 Nmap

nmap - кез-келген нысандар саны бар IP желілерін әр түрлі теңшелетін сканерлеуге, сканерленген желі объектілерінің (порттар мен оларға сәйкес қызметтер) күйін анықтауға арналған тегін қызметтік бағдарлама. Бастапқыда бағдарлама UNIX жүйелері үшін жүзеге асырылды, бірақ қазір көптеген операциялық жүйелер үшін нұсқалар бар [24].

3.2-сурет – Nmap сканерлеу нәтижелері

Nmap UDP, TCP (connect), TCP SYN (жартылай ашық), FTP-proxy (ftp арқылы серпіліс), reverse-ident, ICMP (ping), FIN, ACK, Xmas tree, SYN - және NULL-сканерлеу сияқты көптеген сканерлеу әдістерін қолданады. Nmap сонымен қатар көптеген қосымша мүмкіндіктерді қолдайды, атап айтқанда: TCP/IP стек іздерін қолдана отырып, қашықтағы хосттың операциялық жүйесін анықтау, "көрінбейтін" сканерлеу, кідіріс уақытын динамикалық есептеу және пакеттік беруді қайталау, параллель сканерлеу, параллель ping сауалнамасы арқылы белсенді емес хосттарды анықтау, жалған хосттарды сканерлеу, пакеттік сүзгілердің болуын анықтау, тікелей (portmapper қолданбай) RPC сканерлеу, IP фрагментациясын сканерлеу, SQL Injection осалдықтарын жылдам іздеу, сондай-ақ, сканерленген желілердің IP мекенжайлары мен порт нөмірлерін ерікті түрде көрсету.

Соңғы нұсқаларында Lua — Nmap Scripting Engine (NSE) бағдарламалау тілінде еркін сценарийлер (сценарийлер) жазу мүмкіндігі қосылды.

Сканерлеу тапсырмаларын орындауды жеңілдететін графикалық интерфейстер бар:

- Nmap Front End (Qt)
- zenmap (GTK, Linux) [25].

3.1.2 Django

Django – Python-да жазылған өте танымал және толық жұмыс істейтін серверлік веб-шеңбер.

URL идентификаторы әдетте urls.py файлында болады. төмендегі мысалда салыстырушы жоларалық салыстырулар тізімін (белгілі бір URL шаблондары) және тиісті дисплей функцияларын (view) анықтайды. Егер белгілі бір шаблонға сәйкес келетін URL мекен-жайы бар HTTP сұранысы алынса, онда байланысты дисплей функциясы шақырылып, сұрауға жіберіледі.

```
urlpatterns = [
   path('admin/', admin.site.urls),
   path('book/<int:id>/', views.book_detail, name='book_detail'),
   path('catalog/', include('catalog.urls')),
   re_path(r'^([0-9]+)/$', views.best),
]
```

Дисплей (views) – бұл веб-клиенттерден HTTP сұрауларын қабылдайтын және HTTP жауаптарын қайтаратын веб-қосымшаның жүрегі. Сонымен қатар, олар мәліметтер базасына, визуализация үлгілеріне және т. б. қол жеткізу үшін басқа жақтау ресурстарын пайдаланады.

```
## filename: views.py (Django view functions)

from django.http import HttpResponse

def index(request):
        # HttpRequest алу - сұрау параметрі
        # Сұраныстағы ақпаратты пайдаланып операцияларды орындаңыз.
        # HttpResponse қайтару
        return HttpResponse('Hello from Django!')
```

Django Веб-қосымшалары модельдер деп аталатын Python нысандары арқылы деректерді өңдейді және сұрайды.

Төмендегі код үзіндісі Team нысаны үшін өте қарапайым Django моделін көрсетеді. Team класы models. Model класынан мұра алады. Ол пәрмен атауы мен пәрмен деңгейін таңбалар өрісі ретінде анықтайды және әр жазба үшін сақталатын таңбалардың максималды санын анықтайды. Team_level бірнеше мәндердің бірі болуы мүмкін, сондықтан біз оны таңдау өрісі ретінде анықтаймыз және көрсетілген опциялар мен сақталған деректер арасында әдепкі мәнмен салыстыруды қамтамасыз етеміз.

```
## filename: views.py (Django view functions)

from django.http import HttpResponse

def index(request):
        # HttpRequest алу - сұрау параметрі
        # Сұраныстағы ақпаратты пайдаланып операцияларды орындаңыз.
        # HttpResponse қайтару
        return HttpResponse('Hello from Django!')
```

Django моделі дерекқорды іздеу үшін қарапайым сұрау API ұсынады. Іздеу әр түрлі критерийлерді қолдана отырып, бір уақытта бірнеше өрістерде жүргізілуі мүмкін және күрделі өрнектерді қолдай алады.

```
## filename: views.py

from django.shortcuts import render
from .models import Team

def index(request):
   list_teams = Team.objects.filter(team_level__exact="U09")
   context = {'youngest_teams': list_teams}
```

```
    return render(request, '/best/index.html', context)
```

Код үзіндісі алдыңғы бөлімдегі render () функциясымен шақырылған HTML шаблонының қалай көрінетінін көрсетеді. Бұл шаблон сурет салу кезінде ол жоғарыдағы render () функциясының ішіндегі контекстік айнымалыдағы youngest_teams деп аталатын тізім айнымалысына қол жеткізе алады деген болжаммен жазылған. HTML қаңқасының ішінде алдымен youngest_teams айнымалысының бар-жоғын тексеріп, содан кейін оны циклде қайталайтын өрнек бар. Әр қайталау кезінде шаблон элементіндегі әр команданың team_name мәнін көрсетеді [26].

```
## filename: best/templates/best/index.html

<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>Home page</title>
</head>
<body>
  {% if youngest_teams %}
    <ul>
      {% for team in youngest_teams %}
        <li>{{ team.team_name }}</li>
      {% endfor %}
    </ul>
  {% else %}
    <p>No teams are available.</p>
  {% endif %}
</body>
</html>
```

3.1.3 HTML

HTML-бұл бағдарламалау тілі емес, таңбаларға тегтерді (белгілерді) бекітуге арналған белгілеу тілі [27].

HTML "гипермәтінді белгілеу тілі" дегенді білдіреді, бірақ әр сөздің келесі мағыналары бар:

− гипермәтін... Мәтіндік деректерді, соның ішінде диаграммаларды, суреттерді, аудио және бейнелерді бөлісуге және көруге мүмкіндік беретін жүйе.жай мәтіннен (таңбалардан) тыс мәтіндік деректер;

− таңба... маркаға. Компьютер оқи алатын тегтерді қосу;

− тіл...тілі[28].

HTML құжатының үзінділерінің мысалдары [29]:

 екі тег арасындағы Мәтін — ашу және жабу.
мұнда элемент href атрибутын, яғни еренсілтемені қамтиды.
Бос элементтің мысалы:

Элементтің аты мен атрибут атаулары терілген регистр HTML-де маңызды емес. Элементтер кірістірілген болуы мүмкін [30]. Мысалы, келесі код:

```
<!DOCTYPE html>
<html>
  <head>
    <meta charset="utf-8" />
    <title>HTML Document</title>
  </head>
  <body>
    <p>
      <b>
        Бұл мәтін қалың, <i>және бұл Курсив</i>болады.
      </b>
    </p>
  </body>
</html>
```

Бұл мынадай нәтиже береді:
Бұл мәтін қалың болады, ал бұл Курсив болады.

3.1.4 CSS

CSS – белгілеу тілін қолдана отырып жазылған құжаттың сыртқы түрін сипаттаудың формалды тілі. Оны кез-келген XML құжаттарына қолдануға болады.

CSS ережелері олар сипаттайтын веб-құжаттың өзінде де, CSS кеңейтімі бар сыртқы файлдарда да орналасуы мүмкін [31].

CSS стильдерін олар сипаттайтын веб-құжатқа төрт жолмен қосуға немесе енгізуге болады:

− стиль суреттеуі жеке папкада болғанда, оны <head> бөлігіне қосылған <link> бөлігі арқылы құжатқа қосуға болады;

```
<!DOCTYPE html>
<html>
        <head>
```

```
            .....
            <link rel="stylesheet" type="text/css" href="style.css">
        </head>
        <body>
          .....
        </body>
</html>
```

– стиль құжаты бастапқы құжаттан жеке тұрақталғанда, оны құжатқа <style > бөлігіндегі @import нұсқауымен қосу мүмкін;

```
<!DOCTYPE html>
<html>
         <head>
          .....
            <style media="all">
                  @import url(style.css);
             </style>
        </head>
</html>
```

– мәнерлер құжатта көрсетілген кезде, оларды <head> бөлігіне кіретін <style > бөлігіне қосуға мүмкіндік бар;

```
<!DOCTYPE html>
<html>
          <head>
            .....
          <style>
            body {
                  color: red;
            }
          </style>
        </head>
        <body>
          .....
        </body>
</html>
```

– құжатта үлгілер көрсетілгенде жеке бөліктердің тиесілілігінде тұрақтауы мүмкін [32]:

```
<!DOCTYPE>
<html>
        <head>
```

```
        .....
      </head>
      <body>
        <p style="font-size: 20px; color: green; font-family: arial, helvetica, sans-
    serif">
          .....
        </p>
      </body>
</html>
```

3.1.5 JavaScript

JavaScript, көбінесе қысқартылған JS – бұл HTML және CSS-пен бірге Бүкіләлемдік ғаламтордың негізгі технологияларының бірі болып табылатын бағдарламалау тілі. Веб-сайттардың 97%-дан астамы көбінесе үшінші тарап кітапханаларын қолдана отырып, веб-беттерді жүргізу үшін клиенттік JavaScript қолданады. Барлық негізгі веб-браузерлерде пайдаланушы құрылғыларында кодты орындау үшін арнайы JavaScript қозғалтқышы бар [33].

JavaScript-те кірістірілген енгізу/шығару функциясы жоқ; жұмыс уақыты мұны қамтамасыз етеді. 5.1 редакциясындағы ECMAScript сипаттамасында: шынында да, бұл сипаттамада сыртқы деректерді енгізу немесе есептелген нәтижелерді шығару ережелері жоқ [34].

Алайда, жұмыс ортасының көпшілігінде шығыс деректерін басып шығару үшін пайдалануға болатын консоль нысаны бар. Міне, JavaScript-тегі Hello World минималистік бағдарламасы:

```
console.log(“Hello, world!”);
```

HTML құжаттарында бұл бағдарлама көрсету үшін қажет:

```
// Text nodes can be made using the "write" method.
document.write('foo');

// Elements can be made too. First, they have to be created in the DOM.
const myElem = document.createElement('span');

// Attributes like classes and the id can be set as well
myElem.classList.add('foo');
myElem.id = 'bar';

// For here, the attribute will look like this: <span data-attr="baz"></span>
myElem.setAttribute('data-atrr', 'baz');
```

```
// Finally append it as a child element to the <body> in the HTML
document.body.appendChild(myElem);

// Elements can be imperitavely grabbed with querySelector for one element, or
querySelectorAll for multiple elements that can be loopped with forEach
document.querySelector('.class');
document.querySelector('#id');
document.querySelector('[data-other]');
document.querySelectorAll('.multiple');
```

JavaScript-те нысандар функциялар сияқты жасалады; бұл функция нысаны ретінде белгілі.

Нысан мысалы:

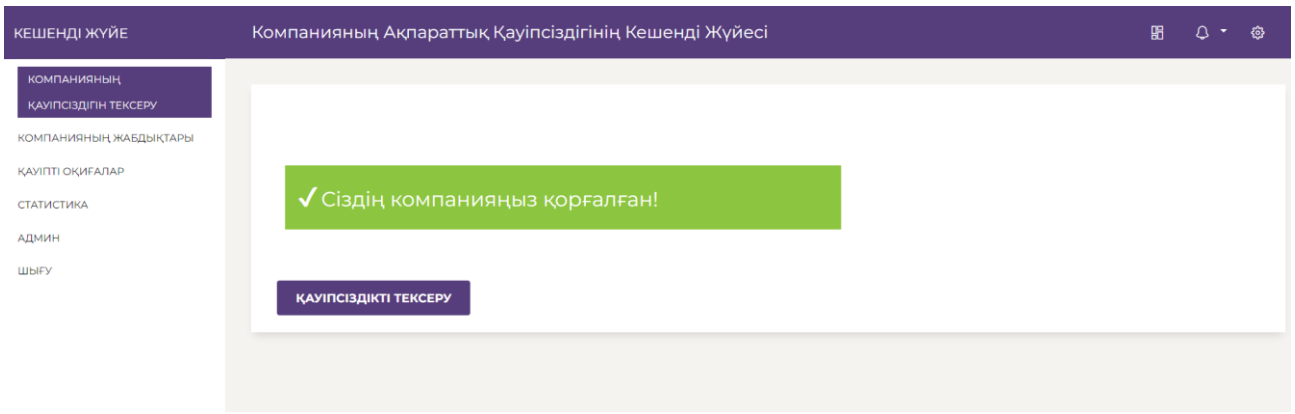
```
function Ball(r) {
   this.radius = r; // the "r" argument is local to the ball object
   this.area = Math.PI * (r ** 2); // parentheses don't do anything but clarify

   // objects can contain functions ("method")
   this.show = function() {
      drawCircle(this.radius); // references another function (that draws a circle)
   };
}

let myBall = new Ball(5); // creates a new instance of the ball object with radius 5
myBall.radius++; // object properties can usually be modified from the outside
myBall.show(); // using the inherited "show" function
```

3.2 Бағдарламаның интерфейсі

Бұл бөлімде бағдарламаның жұмыс істеу тәртібі мен интерфейсіне тоқталатын боламыз.

Бұл бағдарлама компанияның қауіпсіздігін тексеріп отыруға арналған. Scapy және nmap қолдана отырып, компанияның құралдарын, порттарын, IP адрестерін жазып, логин және құпия сөздерін енгізіп қоямыз. Осы scapy және nmap арқылы компанияда болып жатқан қауіпті іс-әрекеттерді көре аламыз. Сканер арқылы компанияның қауіпсіздігін тексерерміз, ал жалпы қауіпті оқиғалар тізімі жеке бөлімде көрсетіліп тұрады.

Жүйеге кіргеннен кейін, басты бетте компанияның соңғы статусы көрсетіліп тұрады (яғни соңғы компания қауіпсіздігін тексерген кездегі жағдайы). Мысалы, 3.3 – суретте компанияның қорғалғаны туралы көрсетілген.

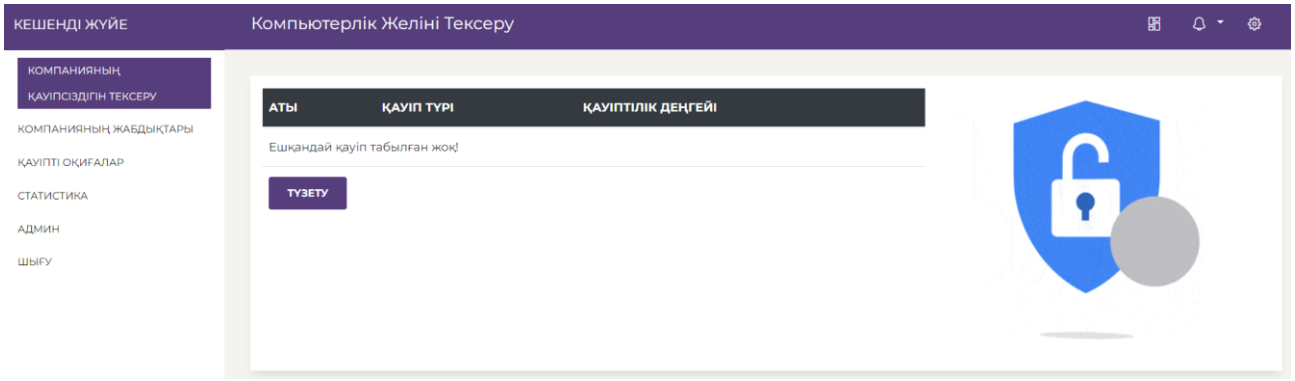


3.3-сурет – Басты бет

Компания қауіпсіздігін жаңадан тексеру үшін «Қауіпсіздікті тексеру» батырмасын басамыз. Сол кезде 3.4 – суретте көрсетілгендей жүйе компанияның қауіпсіздігін тексеруге көшеді.

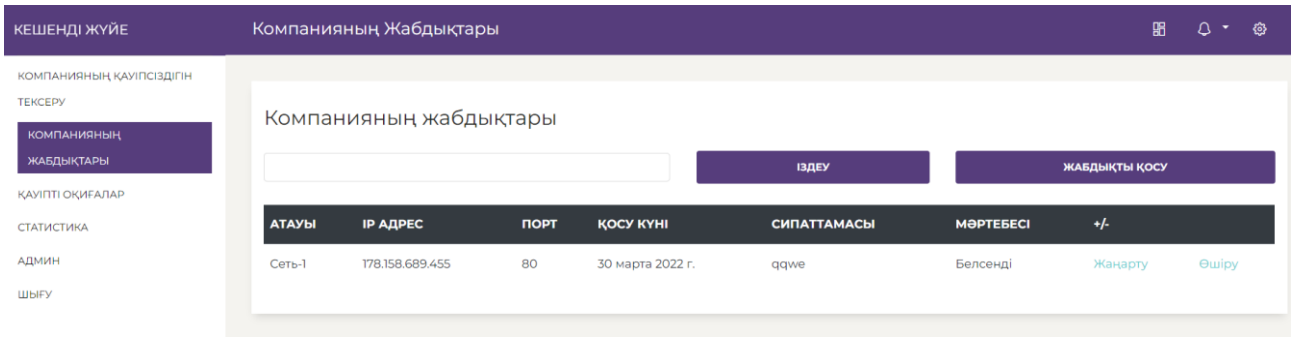
3.4-сурет – Компания қауіпсіздігін тексеру

Тексеріс аяқталғаннан кейін экранға нәтижесі шығады. Егер қауіп бар болса, аты, түрі, деңгейі көрсетіледі. Егер жоқ болса, 3.5 – суреттегідей «Ешқандай қауіп табылған жоқ» мәтіні шығады.



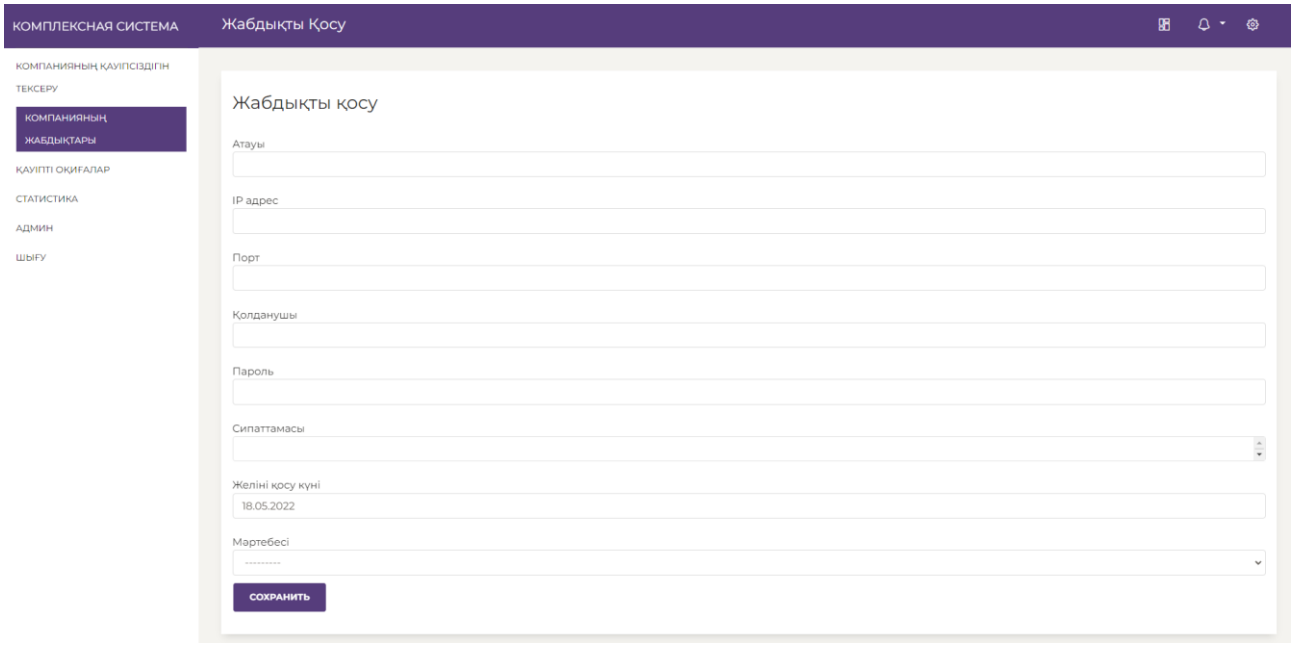
3.5-сурет – Тексеріс нәтижесі

Келесі бөлім «Компанияның жабдықтары». Бұл бетте компания құралдарының тізімі және олар туралы мәліметтер (атауы, IP-адресі, порты, қосылған күні, сипаттамасы, статусы) көрсетіледі. Іздеу жолағына тиісті мәтінді енгізу арқылы керекті құралды тезірек таба аласыз.



3.6-сурет – Компанияның құралдары

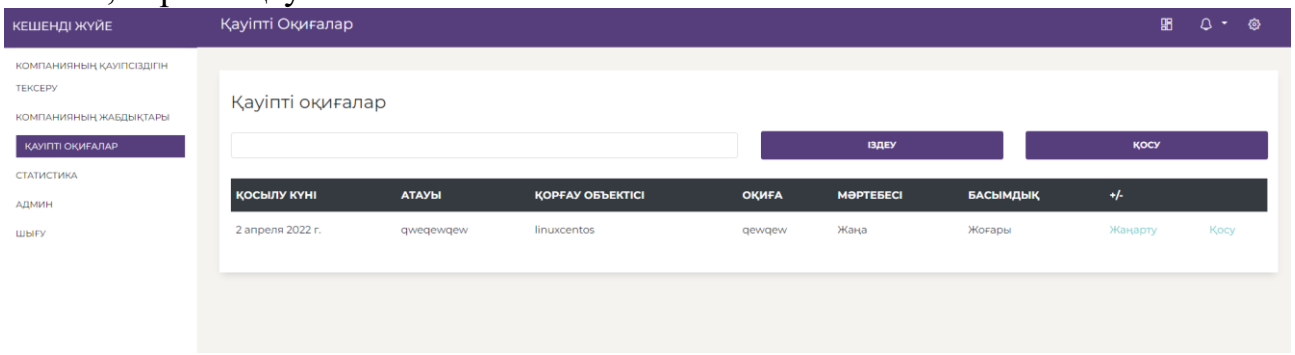
Компания құралдарын жаңадан енгізу үшін «Жабдықты қосу» батырмасын басамыз. Жоғарыда көрсетілген мәліметтерді жаңа құрал үшін енгізіп шығамыз. «Сақтау» батырмасын басамыз. Құрал сақталды.



3.7- сурет – Жаңа құрал қосу

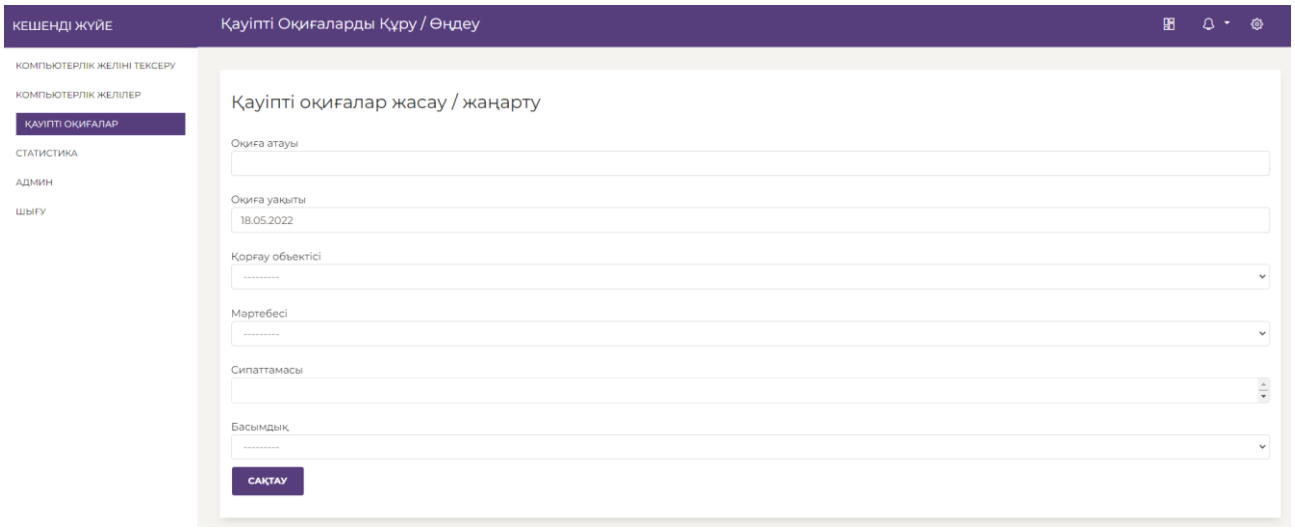
Тексерістен кейінгі анықталған қауіптер тізімі «Қауіпті оқиғалар» бөлімінде көрсетіледі. Бұл бетте қауіптердің аты, қосылу күні, қорғау объектісі,

инциденті, статусы және басымдық көрсетіледі. Іздеу жолағына тиісті мәтінді жазып, керекті қауіпті таба аласыз.



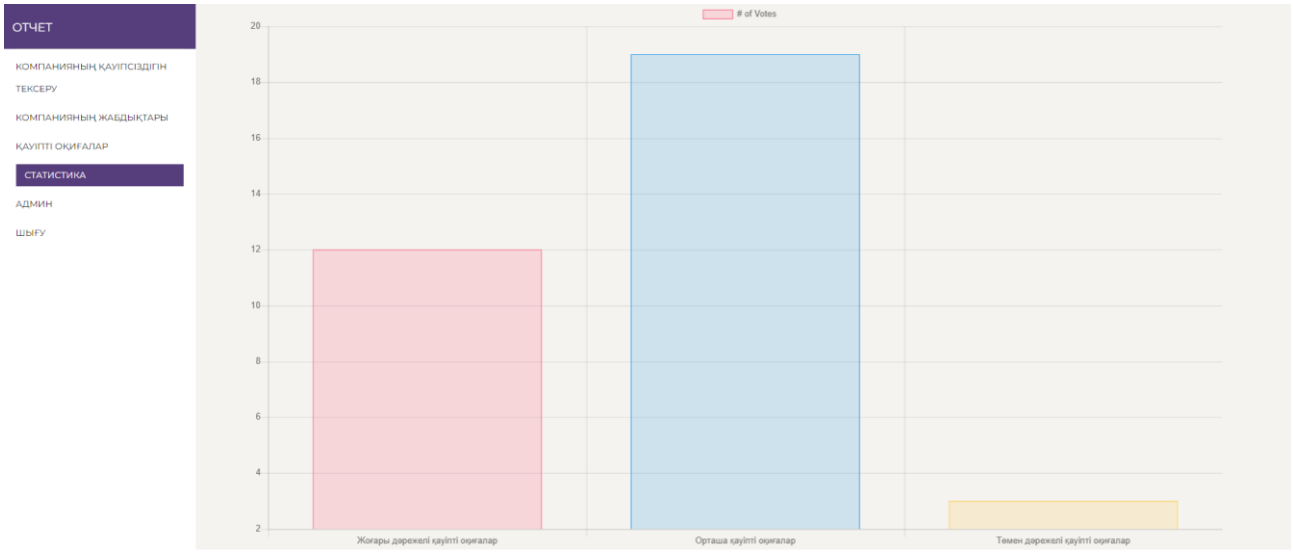
3.8- сурет – Қауіпті оқиғалар

Сондай-ақ пайда болған қауіптерді өзіңіз енгізе аласыз. Жоғарыда көрсетілген мәліметтерін өзіңіз теріп, «сақтау» батырмасын басып, сақтай аласыз.



3.9-сурет – Қауіпті оқиғаны енгізу

Осы жүйе анықтаған барлық қауіп-қатерлер туралы есептілікті «Статистика» бөлімінен көре аласыз.



3.10-сурет – Қауіптілік диаграммасы

ҚОРЫТЫНДЫ

Қорытындылай келе, жасалған жүйеде интерфейсі оның функционалдығы мен пайдалану қарапайымдылығымен сәтті үйлесетінін атап өтуге болады. Қолданушының барынша ыңғайлы және қолжетімді жұмысы, қолжетімді және түсінікті диалогтық терезелер әзірленді.

Деректерді қауіпсіздікте сақтаудың маңызы – ақпараттық деректерді, сондай-ақ қолдау инфрақұрылымын абайсызда немесе әдейі үшінші тұлғалардың қол жеткізуінен қорғау, бұл мәліметтердің жойылуына немесе олардың рұқсатсыз өңделуіне алып келуі мүмкін.

Компанияда ақпараттық қауіпсіздік бағдарламаларын оңтайлы іске қосу үшін үш басты принцип орындалуы керек:

1 Құпиялылық – керексіз немесе меншік иесінің келісімінсіз деректерге қол жеткізудің алдын алу үшін ұйымдағы процесстердің әр сатысындағы мәліметтеріне, активтеріне және деректерінің қауіпсіздігіне сенімді болу үшін бақылауды іске қосуды білдіреді.

2 Тұтастық – ұйымдағы мәліметтердің ішкі және сыртқы сәйкестік болуын орындауға қатысты басқару элементтерімен жүзеге асады.

3 Қол жетімділік – жеке тұлғалардың мәліметтерге қауіпсіз және оңтайлы қолдануын жүзеге асырады. Мәліметтер мен деректерді қолданау үшін кәсіпорын үшін арнайы желілік орта алдын-ала дайындалуы керек.

Дипломдық жобаның мақсаты компания қауіпсіздігінің кешенді жүйесін әзірлеу болатын. Бұл мақсатқа жету үшін диплом жобасы барысында келесі тапсырмалар шешілді: ақпараттық қауіпсіздік түсінігіне теориялық зерттеулер жүргізілді, оның кәсіпорында саласында қолдану ерекшеліктері анықталды, біртұтас бағдарлама құрылып, маңыздылығына талдау жасалынды.

Дипломдық жоба барысында теориялық білімге сүйене отырып, Python программалау тілінде компания қауіпсіздігінің кешенді жүйесі құрылды. Бұл жүйе кәсіпорынның ақпараттарының сақталуына, қызметкерлердің уақытты үнемдеуіне мүмкіндік береді. Бағдарламада компанияның қауіптері туралы ақпарат алуға болады және сол қауіп-қатерлер бойынша есептілік диаграмма түрінде көрсетіледі. Дайындалған бағдарламаның артықшылықтарын атап көрсетсем:

- Функционалдық – бағдарлама көптеген функцияларды атқара алады, бұл өз кезегінде қолданушының сұранысын қамтамасыз ете алады;
- Ауқымдылық – бағдарламаны шексіз көп қолданушы қолдана алады;
- Қарапайым интерфейс – әзірленген автоматтандырылған жүйеде интерфейстің қарапайым және түсінікті формасы, оңай басқарылатын мәзір және мақсаттар мен міндеттерді шешуге арналған барлық қажетті құралдар жиынтығы бар.
- Қолжетімділік – сайтқа кез-келген Интернетке қосылған құрылғы (компьютер, смартфон, планшет) арқылы кіруге болады.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1 Основные понятия информационной безопасности. URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/osnovnye-aspekty-informatsionnoj-bezopasnosti/osnovnye-ponyatiya-informatsionnoj-bezopasnosti/ https://scienceon.kisti.re.kr/srch/selectPORSrchReport.do?cn=KAR2013070025&dbt=RESEAT#:~:text=%E2%97%8B%20%EC%A0%95%EB%B3%B4%EB%B3%B4%EC%95%88%EC%9D%98%20%EA%B0%9C%EB%85%90,%EA%B8%B0%EC%88%A0%EC%A0%81%20%EB%B0%A9%EB%B2%95%EC%9D%84%20%EC%9D%98%EB%AF%B8%ED%95%9C%EB%8B%A4.

2 *Алексей Лукацкий.* Триада \"конфиденциальность, целостность, доступность\": откуда она? // SecurityLab.ru.— 2012. — 20 сентября.

3 *Olavsrud, Thor*. 5 information security threats that will dominate 2018: // CIO.com. Дата обращения: 13 января 2019. — IDG Communications, Inc., 2017. — 20 November.

4 *Stewart, James Michael.* CISSP: Certified Information Systems Security Professional Study Guide: / James Michael Stewart, Mike Chapple, Darril Gibson. — Seventh Edition. — Canada: John Wiley & Sons, Inc., 2015. — 1023p.

5 *Andress J.*The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. — Syngress, 2014. — 240p.

6 Информационная безопасность - Материал из Википедии - 12 ноября 2021. URL: https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C

7 Основные принципы обеспечения информационной безопасности – SearchInform. URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/osnovnye-aspekty-informatsionnoj-bezopasnosti/osnovnye-printsipy-obespecheniya-informatsionnoj-bezopasnosti/

8 Принципы информационной безопасности. URL:https://arinteg.ru/articles/printsipy-informatsionnoy-bezopasnosti-26490.html

9 Информационная безопасность на предприятии: с чего начать - SearchInform - 21.01.2020 - URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/informatsionnaya-bezopasnost-v-otraslyakh/informatsionnaya-bezopasnost-predpriyatij/informatsionnaya-bezopasnost-na-predpriyatii-s-chego-nachat/

10 Примеры информационной безопасности предприятия - SearchInform - 06.02.2020 - URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/informatsionnaya-bezopasnost-v-otraslyakh/informatsionnaya-bezopasnost-predpriyatij/primery-informatsionnoj-bezopasnosti-predpriyatiya/

11 Обеспечение информационной безопасности предприятий торговли, торговых сетей и их инфраструктуры - Сайт ITSec.Ru-2007 - Сергей Русинов - URL: https://lib.itsec.ru/articles2/Inf_security/infosec-torg

12 Комплексные системы обеспечения информационной безопасности - SearchInform - 04.02.2020 - URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/informatsionnaya-bezopasnost-v-otraslyakh/bezopasnost-informatsionnykh-sistem/kompleksnye-sistemy-obespecheniya-informatsionnoj-bezopasnosti/

13 *Мельников В.П., Клейменов С.А.*Информационная безопасность и защита информации. М.: Академия, 2009.

14 *Щербаков Л.Ю.* Современная компьютерная безопасность. Теоретические основы. Практические аспекты. М.: Книжный мир, 2009.

15 Комплексное обеспечение информационной безопасности - Основные положения информационной безопасности - 2018 - URL: https://studref.com/306315/informatika/kompleksnoe_obespechenie_informatsionnoy_bezopasnosti

16 Средства обеспечения информационной безопасности - Артем П. - 08.11.20. URL: https://cisoclub.ru/sredstva-obespecheniya-informaczionnoj-bezopasnosti/

17 Программно-аппаратная защита информации - SearchInform - 08.11.2019. URL: https://searchinform.ru/services/outsource-ib/zaschita-informatsii/programmno-apparatnaya/

18 Техническое обеспечение информационной безопасности предприятия - SearchInform -04.02.2020. URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/informatsionnaya-bezopasnost-v-otraslyakh/informatsionnaya-bezopasnost-predpriyatij/tekhnicheskoe-obespechenie-informatsionnoj-bezopasnosti-predpriyatiya/

19 Способы защиты информации - SearchInform - 2020. URL: https://searchinform.ru/informatsionnaya-bezopasnost/zaschita-informatsii/sposoby-zaschity-informatsii/

20 Методы защиты информации - Мария Константиновна Коваленко - 10.03.2019. URL: https://spravochnick.ru/informacionnaya_bezopasnost/zaschita_informacii/metody_zaschity_informacii/

21 Yogesh Rana. Python: Simple though an Important Programming language // International Research Journal of Engineering and Technology (IRJET). — 2019. — 2 February (vol.06, iss.2). P. 1856—1858.

22 *Ноа Гифт, Джереми М.Джонс*. Python в системном администрировании UNIX и Linux. — СПб: Символ-плюс, 2009.— С.511

23 Scapy – Википедиядан алынған материал – 24 қаңтар 2021. URL: https://ru.wikipedia.org/wiki/Scapy

24 *Lyon G., Lyon G. F.* Nmap 7.92 Defcon Release! — 2021.

25 nmap – Википедиядан алынған материал – 7 наурыз 2022. URL: https://ru.wikipedia.org/wiki/Nmap

26 Изучение веб-разработки. Django введение. // URL: https://developer.mozilla.org/ru/docs/Learn/Server-side/Django/Introduction

27 HTMLとは？基本のタグやできることを世界一わかりやすく解説！ - 18.11.2021. // URL: https://www.sejuku.net/blog/6026

28 HTML – Материал из Википедии. – 09.05.2022. // URL: https://ru.wikipedia.org/wiki/HTML#:~:text=HTM.

29 Питер Лабберс, Брайан Олберс, Фрэнк Салим. HTML5 для профессионалов: мощные инструменты для разработки современных веб-приложений = Pro HTML5 Programming: Powerful APIs for Richer Internet Application Development. —М.: «Вильямс», 2011.— 272б.

30 CSS – Материал из Википедии. – 05.05.2022. // URL: https://ru.wikipedia.org/wiki/CSS

31 Дэвид Сойер Макфарланд. Новая большая книга CSS = CSS: The Missing Manual.— Санкт-Петербург:Питер, 2017.— 720с.—1000 экз.

32 Flanagan, David. *JavaScript: the definitive guide*. Beijing; Farnham: O'Reilly. p.1

33 JavaScript – Материал из Википедии - 14 марта 2022. URL: https://en.wikipedia.org/wiki/JavaScript

34 Flanagan, David. *JavaScript: The Definitive Guide*. 7th edition. Sebastopol, California: O'Reilly, 2020.

А қосымша
Бағдарлама листингі

```
import nmap3
from scapy.all import *

from .models import (
   Protection,
   Incident
)

class NmapScanner(object):

   def perform_full_scan_and_save(self, target, args="-A"):

      nmap = nmap3.Nmap()
      scanner_result = nmap.nmap_version_detection(target, args=args)

      scanner_history = ScannerHistory(
         target=target,
         type='FS'
      )

      scanner_history.save()

      IPList = list(scanner_result)

      for IP in IPList:

         host_data = {
            'IP': IP
         }
         if "macaddress" in scanner_result[IP]:

            if scanner_result[IP]["macaddress"] is not None:

               if "addr" in scanner_result[IP]["macaddress"]:
                  host_data['mac_address'] = scanner_result[IP]["macaddress"]["addr"]

         host, created = Host.objects.get_or_create(**host_data)
         scanner_history.hosts.add(host)

         if "osmatch" in scanner_result[IP]:
            for osmatch in scanner_result[IP]["osmatch"]:
```

А қосымшасының жалғасы

```
            operative_system_match,                    created                    =
OperativeSystemMatch.objects.get_or_create(
                name=osmatch["name"],
                accuracy=osmatch["accuracy"],
                line=osmatch["line"],
                host=host
            )

            if "osclass" in osmatch:

                operative_system_class_data = {}

                operative_system_class_data['operative_system_match']              =
operative_system_match

                if "type" in osmatch["osclass"]:
                    operative_system_class_data['type'] = osmatch["osclass"]["type"]

                if "vendor" in osmatch["osclass"]:
                    operative_system_class_data['vendor']                          =
osmatch["osclass"]["vendor"]

                if "osfamily" in osmatch["osclass"]:
                    operative_system_class_data['operative_system_family']         =
osmatch["osclass"]["osfamily"]

                if "osgen" in osmatch["osclass"]:
                    operative_system_class_data['operative_system_generation']     =
osmatch["osclass"]["osgen"]

                if "accuracy" in osmatch["osclass"]:
                    operative_system_class_data['accuracy']                        =
osmatch["osclass"]["accuracy"]

                operative_system_class,                    created                 =
OperativeSystemClass.objects.get_or_create(
                    **operative_system_class_data
                )

        if "ports" in scanner_result[IP]:
            for ports in scanner_result[IP]["ports"]:
```

А қосымшасының жалғасы

```
                port = Port(
                    protocol=ports["protocol"],
                    portid=ports["portid"],
                    state=ports["state"],
                    reason=ports["reason"],
                    reason_ttl=ports["reason_ttl"],
                    host=host
                )

                port.save()

                if "service" in ports:
                    port_service_data = {}

                    port_service_data['port'] = port

                    if "name" in ports["service"]:
                        port_service_data['name'] = ports["service"]["name"]

                    if "product" in ports["service"]:
                        port_service_data['product'] = ports["service"]["product"]

                    if "extrainfo" in ports["service"]:
                        port_service_data['extra_info'] = ports["service"]["extrainfo"]

                    if "hostname" in ports["service"]:
                        port_service_data['hostname'] = ports["service"]["hostname"]

                    if "ostype" in ports["service"]:
                        port_service_data['operative_system_type'] =
ports["service"]["ostype"]

                    if "method" in ports["service"]:
                        port_service_data['method'] = ports["service"]["method"]

                    if "conf" in ports["service"]:
                        port_service_data['conf'] = ports["service"]["conf"]

                    port_service = PortService(
                        **port_service_data
                    )
```

А қосымшасының жалғасы

```
                port_service.save()

        return scanner_history


class ScapyScanner(object):

    def __init__(self):
        self.target = None
    def save_quick_scan(self):
        answered, unanswered = arping(self.target)

        scanner_history = ScannerHistory(
            target=self.target
        )

        scanner_history.save()

        for row in answered:

            original_packet, answer = row

            IP = answer.psrc
            mac_address = answer.hwsrc

            host, created = Host.objects.get_or_create(
                IP=IP,
                mac_address=mac_address
            )
            scanner_history.hosts.add(host)

        return scanner_history



from datetime import datetime
from django.db import models

class Status(models.Model):
    title = models.CharField(max_length=240, verbose_name = 'Название')

    def __str__(self):
```

```
        return self.title


    class Meta:
        verbose_name = "Статус"
        verbose_name_plural = "Статус"

class Protection(models.Model):
    title = models.CharField(max_length=240, verbose_name = 'Защита')

    def __str__(self):
        return self.title

    class Meta:
        verbose_name = "Защита компании"
        verbose_name_plural = "Защита компании"

class Priority(models.Model):
    title = models.CharField(max_length=240)
    def __str__(self):
        return self.title

    class Meta:
        verbose_name = "Приоритет"
        verbose_name_plural = "Приоритет"

# инцидент
class Incident(models.Model):
    title = models.CharField(max_length=240)
    date_discovery = models.DateField(default=datetime.now)
    protection = models.ForeignKey(Protection, on_delete=models.CASCADE)
    status = models.ForeignKey(Status, on_delete=models.CASCADE)
    data_pk = models.TextField(max_length=240)
    priority = models.ForeignKey(Priority, on_delete=models.CASCADE)

    def __str__(self):
        return self.title

    class Meta:
        verbose_name = "Событие"
        verbose_name_plural = "Событие"
```

А қосымшасының жалғасы

```
# Типы опасности
class TypeVirus(models.Model):
    title = models.CharField(max_length=240)


    def __str__(self):
        return self.title


# Опасность
class Danger(models.Model):
    DANGER_LEVEL_CHOICES = [
        ('Низкий', 'Низкий'),
        ('Средний', 'Средний'),
        ('Высоко', 'Высоко'),
        ('Очень высоко', 'Очень высоко')
    ]
    title = models.CharField(max_length=240)
    type_virus = models.ForeignKey(TypeVirus, on_delete=models.CASCADE, null=True)
    danger_level = models.CharField(max_length=240, choices=DANGER_LEVEL_CHOICES)
    description = models.TextField(null=True, blank=True)

    def __str__(self):
        return self.title

    class Meta:
        verbose_name = "Опасность"
        verbose_name_plural = "Опасность"
```

РЕЦЕНЗИЯ

на дипломную работу студента 4 курса Казахского национального исследовательского технического университета им. К.И.Сатпаева специальности 5В070300 «Информационные системы»

Кадекешова Бекзата Тулебайулы

на тему: «Проектирование комплексной системы информационной безопасности компании»

Целью дипломной работы является проектирование комплексной системы информационной безопасности компании.

Дипломный проект состоит из введения, трех глав, заключения, списка литературы и приложения. Во введении кратко изложены значимость проблемы, цель работы и задачи. В первом разделе изложены понятия информационной безопасности, перечислены средства обеспечения информационной безопасности. Во втором разделе показана блок-схема комплексной системы безопасности предприятия, а также программная реализация поставленной задачи работы описана в третьем разделе.

Автором работы при выполнении были использованы компьютерные технологии, в частности, база данных была скомпилирована в среде Python, а пользовательский интерфейс реализован через визуальные компоненты Django.

Данная работа содержит некоторые недостатки, например, небольшой объем введения, не раскрыта актуальность, цели и задачи дипломного проекта. Изложенный текст в исследовании не полностью раскрывает результаты исследования.

Автор работы во время выполнения дипломной работы использовал труды зарубежных ученых, это подтверждается списком использованных литератур.

Дипломный проект соответствует требованиям, предъявляемым к выпускным работам по специальности 5В070300.

Выпускная работа Кадекешова Б.Т. заслуживает «75 хорошо» оценки и присвоения его исполнителю квалификацию «бакалавр» по специальности 5В070300 «Информационные системы».

Рецензент
Доктор PhD, главный ученый секретарь, СНС «Института информационных и вычислительных технологий КН МОН РК _____ **Усатова О. А.**

«20» мая **2022 г.**

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
СӘТБАЕВ УНИВЕРСИТЕТІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Мамандығы 5В070300 – «Ақпараттық жүйелер»

Кадекешов Бекзат Тулебайулы

Тақырыбы: «Кәсіпорында ақпараттық қауіпсіздіктің кешенді жүйесін құру»

ҒЫЛЫМИ ЖЕТЕКШІНІҢ СЫН-ПІКІРІ

Кәсіпорындағы ақпаратты кешенді қорғауды зерттеудің өзектілігі стандартты режимде жұмыс істейтін автоматтандырылған жүйені рұқсатсыз басқару әсерлерінен және үшінші тұлғалардың ұрлау немесе тұтастығын бұзу мақсатында айналымдағы ақпаратқа қол жетімділігін шектеу қажеттілігімен байланысты. Кадекешов Бекзаттың дипломдық жұмысы компанияның ақпараттық қауіпсіздігінің кешенді жүйесін жобалауға арналған.

Дипломдық жұмыста ақпараттық қауіпсіздік түсінігіне теориялық зерттеулер жүргізілді, кәсіпорынның ақпараттық қауіпсіздігін қамсыздандыру ерекшеліктері анықталды, ақпаратты қорғау әдістері талданылды.

Дипломдық жұмыстың авторы жұмысты орындау барысында шетелдік ғалымдардың еңбектерін пайдаланды, бұл пайдаланылған әдебиеттер тізімімен расталады.

Дипломдық жоба 5В070300 – «Ақпараттық жүйелер» мамандығы бойынша бітіру жұмыстарына қойылатын талаптарға сәйкес келеді, Кадекешов Б.Т. «бакалавр» академиялық дәрежесін тағайындауға және «жақсы» деген бағаға лайықты деп есептеймін.

ҒЫЛЫМИ ЖЕТЕКШІ
PhD докторы, қауым.профессор _____ Бегимбаева Е.Е.

Кафедра меңгерушісінің ұқсастық есебін талдау хаттамасы

Кафедра меңгерушісі көрсетілген еңбекке қатысты дайындалған Плагиаттың алдын алу және анықтау жүйесінің толық ұқсастық есебімен танысқанын мәлімдейді:

Автор: Кадекешов Б.Т.

Тақырыбы: Компанияның ақпараттық қауіпсіздігінің кешенді жүйесін құру

Координатор: Бегимбаева Е.Е.

1-ұқсастық коэффициенті (30): 3,50

2-ұқсастық коэффициенті (5): 2,74

Әріптерді ауыстыру: 5

Аралықтар: 0

Шағын кеңістіктер: 25

Ақ белгілер: 0

Кафедра меңгерушісі келесі шешімдерді мәлімдейді :

☑ Ғылыми еңбекте табылған ұқсастықтар плагиат болып есептелмейді. Осыған байланысты жұмыс өз бетінше жазылған болып санала отырып, қорғауға жіберіледі.

☐ Осы жұмыстағы ұқсастықтар плагиат болып есептелмейді, бірақ олардың шамадан тыс көптігі еңбектің құндылығына және автордың ғылыми жұмысты өзі жазғанына қатысты күмән тудырады. Осыған байланысты ұқсастықтарды шектеу мақсатында жұмыс қайта өңдеуге жіберілсін.

☐ Еңбекте анықталған ұқсастықтар жосықсыз және плагиаттың белгілері болып саналады немесе мәтіндері қасақана бұрмаланып плагиат белгілері жасырылған. Осыған байланысты жұмыс қорғауға жіберілмейді.

Негіздеме:

Күні:

КАӨжС кафедрасы меңгерушісі
т.ғ.к., қауым. профессор
_____Р.Ж.Сатыбалдиева

Ғылыми жетекшінің ұқсастық есебіне талдау хаттамасы

Ғылыми жетекші көрсетілген еңбекке қатысты дайындалған Плагиаттың алдын алу және анықтау жүйесінің толық ұқсастық есебімен танысқанын мәлімдейді:

Автор: Кадекешов Б.Т.

Тақырыбы: Компанияның ақпараттық қауіпсіздігінің кешенді жүйесін құру

Координатор: Бегимбаева Е.Е.

1-ұқсастық коэффициенті (30): 3,50

2-ұқсастық коэффициенті (5): 2,74

Әріптерді ауыстыру: 5

Аралықтар: 0

Шағын кеңістіктер: 25

Ақ белгілер: 0

Ғылыми жетекші келесі шешімдерді мәлімдейді :

☑ Ғылыми еңбекте табылған ұқсастықтар плагиат болып есептелмейді. Осыған байланысты жұмыс өз бетінше жазылған болып санала отырып, қорғауға жіберіледі.

☐ Осы жұмыстағы ұқсастықтар плагиат болып есептелмейді, бірақ олардың шамадан тыс көптігі еңбектің құндылығына және автордың ғылыми жұмысты өзі жазғанына қатысты күмән тудырады. Осыған байланысты ұқсастықтарды шектеу мақсатында жұмыс қайта өңдеуге жіберілсін.

☐ Еңбекте анықталған ұқсастықтар жосықсыз және плагиаттың белгілері болып саналады немесе мәтіндері қасақана бұрмаланып плагиат белгілері жасырылған. Осыған байланысты жұмыс қорғауға жіберілмейді.

Негіздеме:

Күні:

Ғылыми жетекшісі
Ph.D докторы, қауым. профессор
_____Бегимбаева Е.Е.

StrikePlagiarism.com | SATBAYEV UNIVERSITY

Дата отчета 5/16/2022
Дата редактирования —

Отчет не был оценен

Метаданные

Название
диплом_Кадекешов_Бекзат.docx

Автор
Кадекешов Бекзат Научный руководитель

Подразделение
ИАиИТ

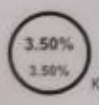
Список возможных попыток манипуляций с текстом

В этом разделе вы найдете информацию, касающуюся манипуляций в тексте, с целью изменить результаты проверки. Для того, кто оценивает работу на бумажном носителе или в электронном формате, манипуляции могут быть невидимы (может быть также целенаправленное вписывание ошибок). Следует оценить, являются ли изменения преднамеренными или нет.

Замена букв		5
Интервалы		0
Микропробелы		25
Белые знаки		0
Парафразы (SmartMarks)		7

Объем найденных подобий

Обратите внимание!Высокие значения коэффициентов не означают плагиат. Отчет должен быть проанализирован экспертом.



КП1

КП2

КЦ

25
Длина фразы для коэффициента подобия 2

5737
Количество слов

49275
Количество символов

Подобия по списку источников

Просмотрите список и проанализируйте, в особенности, те фрагменты, которые превышают КП №2 (выделенные жирным шрифтом). Используйте ссылку «Обозначить фрагмент» и обратите внимание на то, являются ли выделенные фрагменты повторяющимися короткими фразами, разбросанными в документе (совпадающие сходства), многочисленными короткими фразами расположенные рядом друг с другом (парафразирование) или обширными фрагментами без указания источника ("криптоцитаты").

10 самых длинных фраз | Цвет текста

ПОРЯДКОВЫЙ НОМЕР	НАЗВАНИЕ И АДРЕС ИСТОЧНИКА URL (НАЗВАНИЕ БАЗЫ)	КОЛИЧЕСТВО ИДЕНТИЧНЫХ СЛОВ (ФРАГМЕНТОВ)	
1	https://topuch.ru/mamandii-vtipo-18-4a-sj-tairibi-bailau-jmisi-orindaan/index.html	115	2.00 %
2	https://topuch.ru/mamandii-vtipo-18-4a-sj-tairibi-bailau-jmisi-orindaan/index.html	42	0.73 %
3	https://stud.kz/referat/show/105266	17	0.30 %
4	https://topuch.ru/mamandii-vtipo-18-4a-sj-tairibi-bailau-jmisi-orindaan/index.html	14	0.24 %
5	Разработка программной системы мониторинга состояния кластерной гибридной вычислительной системы [redacted] 5/25/2021 Yessenov University (Yessenov University)	13	0.23 %

из базы данных RefBooks (0.00 %)

ПОРЯДКОВЫЙ НОМЕР	НАЗВАНИЕ	КОЛИЧЕСТВО ИДЕНТИЧНЫХ СЛОВ (ФРАГМЕНТОВ)

из домашней базы данных (0.00 %)

ПОРЯДКОВЫЙ НОМЕР	НАЗВАНИЕ	КОЛИЧЕСТВО ИДЕНТИЧНЫХ СЛОВ (ФРАГМЕНТОВ)

из программы обмена базами данных (0.23 %)

ПОРЯДКОВЫЙ НОМЕР	НАЗВАНИЕ	КОЛИЧЕСТВО ИДЕНТИЧНЫХ СЛОВ (ФРАГМЕНТОВ)	
1	Разработка программной системы мониторинга состояния кластерной гибридной вычислительной системы [redacted] 5/25/2021 Yessenov University (Yessenov University)	13 (1)	0.23 %

из интернета (3.28 %)

ПОРЯДКОВЫЙ НОМЕР	ИСТОЧНИК URL	КОЛИЧЕСТВО ИДЕНТИЧНЫХ СЛОВ (ФРАГМЕНТОВ)	
1	https://topuch.ru/mamandii-vtipo-18-4a-sj-tairibi-bailau-jmisi-orindaan/index.html	171 (3)	2.98 %
2	https://stud.kz/referat/show/105266	17 (1)	0.30 %

Список принятых фрагментов (нет принятых фрагментов)

ПОРЯДКОВЫЙ НОМЕР	СОДЕРЖАНИЕ	КОЛИЧЕСТВО ИДЕНТИЧНЫХ СЛОВ (ФРАГМЕНТОВ)