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

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

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: «Әлеуметтік инженерия ақпараттық қауіпсіздік аспектісінде» пәні бойынша зертханалық жұмыстар әдістемесін әзірлеу

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

Алматы 2020

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

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

Дипломдық жобаны орындауға берілген
ТАПСЫРМА

Студент: Қалиев Даулет Жанатұлы
(аты-жөні)

Жобаның тақырыбы: «Әлеуметтік инженерия ақпараттық қауіпсіздік аспектісінде» пәні бойынша зертханалық жұмыстар әдістемесін әзірлеу

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

Аяқталған жұмысты тапсыру мерзімі: «____»_____20___ ж.

Жобаға алғашқы деректер (талап етілетін зерттеу (жоба) нәтижелерінің параметрлері және зерттеу нысанының алғашқы деректері): _____
Әлеуметтік инженерияның бірнеше шабуыл тәсілдері тәжірибе жүзінде іске асырылып, алынған деректерге сүйене отырып, қорғану немесе алдын алу жолдары ұсынылды. Атап айтқанда, әлеуметтік желі пайдаланушысының сеніміне кіру және ақпаратқа қол жеткізу, фишинг сайт, Кви кво про әдісі, және бейнебақылауды басқару. Осы ретте iVMS 4200, «NESCA-3» жабық ақпарат көздерінің бағдарламалары пайдаланылды.

Диплом жобасындағы әзірленуі тиіс мәселелер тізімі немесе диплом жобасының қысқаша мазмұны:_____
1. Әлеуметтік инженерияның өзектілігі.
2. Әлеуметтік инженерияның әдістері.
3. Әлеуметтік инженерияға іс жүзінде эксперимент жасау.
4. Әлеуметтік инженериядан қорғану немесе алдын алу жолдарын әзірлеу.
5. Жұмыс жағдайында табиғи жарықтандыруды, өрт қауіпсіздігін және хабарлағаш санын есептеу.
6. Ақпараттық қауіпсіздік тәуекелдерін екі параметр бойынша бағалау.

Графикалық материалдардың (міндетті түрде дайындалатын сызбаларды көрсету) тізімі:

3.3 сурет – Қол жеткізілген құжат (JPG форматта)

3.6 сурет – Қолданылған ұялы телефон жайында ақпарат

3.9 сурет – Қол жеткізілген құпия деректер

3.17 сурет – Вирус туралы хабарлама

3.24 сурет – Құпия сөзді қате және дұрыс енгізудің нәтижелері

3.35 сурет – Бейнебақылауды басқару нәтижесі

4.1- кесте – Жасанды жарықтану кезіндегі жарықтандыру нормалары және табиғи мен қосарлы жарықтану кезіндегі ТЖК

4.4-кесте – ОПУ-8 өрт сөндіргішінің сипаттамалары

5.3 кесте – Тәуекелдерді бағалаудың қорытынды кестесі

Негізгі ұсынылатын әдебиеттер:

1. Сиротский А.А. Технологии социальной инженерии как потенциальная угроза в социальной сфере. В сборнике: Информационная безопасность бизнеса и общества Сборник избранных статей научно-педагогического состава кафедры информационных систем, сетей и безопасности. Российский государственный социальный университет. – М.: Изд-воВМиК МГУ, 2016. – 67 с.

2. Шудрова К. Социальная инженерия в информационной безопасти. – М.: Изд-во ГЛТ, 2012. – №10. – с. 13-17.

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

Жоба бойынша жобаның бөлімдеріне қатысты белгіленген кеңесшілер

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

Диплом жобасын дайындау
КЕСТЕСІ

Бөлімдердің атауы, әзірленетін мәселелердің тізімі	Ғылыми жетекшіге ұсыну мерзімдері	Ескерту
Кіріспе	12.02.20 – 14.02.20	орындалды
1.1 Әлеуметтік инженерияның өзектілігі	18.02.20 – 10.03.20	орындалды
1.2 Әлеуметтік инженерияның пайда болу уақыты, тарихы	18.02.20 – 10.02.20	орындалды
2 Әлеуметтік инженерия әдістері	12.03.20 – 24.03.20	орындалды
3 Әлеуметтік инженерияға іс жүзінде эксперимент жасау	26.03.20 – 15.04.20	орындалды
4 Өміртіршілік қауіпсіздігі	19.04.20 – 15.05.20	орындалды
4.1 Кәсіпорындағы еңбек жағдайларын талдау	19.04.20 – 02.05.20	орындалды
4.2 Есептеу бөлімі	02.05.20 – 15.05.20	орындалды
5 Ақпараттық қауіпсіздіктің тәуекелдерін есептеу	08.05.20 – 28.05.20	орындалды
5.1 Ақпараттық қауіпсіздік тәуекелдері	08.05.20 – 15.05.20	орындалды
5.2 Екі параметр бойынша есептеу	15.05.20 – 28.05.20	орындалды

Тапсырманың берілген уақыты «12 » қаңтар 2020 ж.

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

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

Орындалатын тапсырманы
қабылдаған студент _____ (Қалиев Д. Ж.)
(қолы) (аты-жөні)

Аңдатпа

Дипломдық жоба құпия ақпаратқа қол жеткізу үшін адамдарды манипуляциялауда қолданылатын әлеуметтік инженерияның әдістері мен мүмкіндіктерін анықтауға арналған. Әлеуметтік инженерия психология мен адам факторының білімін қолданады. Осы ретте шабуыл түрлеріне талдау жасалып, эксперимент жүзінде іске асырылды. Нәтижесінде ұйымның өмір бойы қауіпсіздігін арттыратын әлеуметтік инженериядан ақпаратты қорғау әдістері ұсынылды.

Келесі бөлімдерде әлеуметтік инженерия тәсілдері арқылы неғұрлым басым шабуыл жасалынатын ресурстардың тәуекелдері бағаланып, қорғаныс амалдары ұсынылды және өміртіршілік қауіпсіздігі мәселелері қарастырылды.

Аннотация

Дипломный проект предназначен для определения методов и возможностей социальной инженерии, используемых для манипулирования людьми для доступа к конфиденциальной информации. Социальная инженерия использует знания психологии и человеческого фактора. В связи с этим виды атак были проанализированы и реализованы экспериментально. В результате были предложены методы защиты информации от социальной инженерии, повышающие безопасность организации на протяжении всей жизни.

В следующих разделах были оценены риски наиболее приоритетных атакуемых ресурсов с помощью методов социальной инженерии, предложены защитные меры и рассмотрены вопросы безопасности жизнедеятельности.

Annotation

The diploma project is designed to identify the methods and capabilities of social engineering used to manipulate people to access confidential information. Social engineering uses knowledge of psychology and the human factor. In this regard, the types of attacks were analyzed and implemented experimentally. As a result, methods were proposed to protect information from social engineering, which increase the security of the organization throughout life.

In the following sections, the risks of the most priority attacked resources were assessed using social engineering methods, protective measures were proposed, and issues of life safety were considered.

Мазмұны

Кіріспе

Қазіргі өмірдің барлық салаларында компьютерлік жүйелерді қолдану, желілік технологиялардың қарқынды дамуы, артықшылықтардан басқа, көптеген нақты мәселелердің туындауына әкелді. Мұндай мәселелердің бірі ақпаратты тиімді қорғауды қамтамасыз ету қажеттілігі болып табылады, ол ұрлықпен және компьютерлік жүйелердің жадында сақталатын және байланыс желілері бойынша берілетін деректерге заңсыз қол жеткізумен құқық бұзушылықтардың өсуіне байланысты.

Бүгінгі таңда бүкіл әлемде кездесетін компьютерлік қылмыстар адам қызметінің көптеген салаларында жиі кездеседі. Бұл қылмыстар жоғары құпиялылықпен, оларды жасаудың анықталған фактілері бойынша дәлелдер жинаудың қиындықтарымен және мұндай істерді сотта қарау кезінде дәлелдемелердің күрделілігімен сипатталады.

Шетелдік сарапшылардың деректері бойынша, әр апта сайын әлемде 55 миллионнан астам түрлі компьютерлік бұзулар тіркеледі. Хакерлік шабуыл салдарынан пайдаланушыларға келтірілген шығын мөлшері жыл сайын артып келеді. Өкінішке орай, мұндай қауіп төндіретін статистика компаниялардың және дербес компьютерлердің пайдаланушыларының үлкен санына компьютерлік қауіпсіздіктің кез келген ережелерін елемеуге кедергі келтірмейді. Сарапшылардың бағалауы бойынша, әлемде кеңсе қызметкерлерінің тек 1%-ы дербес компьютерді пайдаланудың корпоративтік ережелерін ұстанады. Бұл жағдай кейбір ақпараттық қатерлерді жүзеге асыру мүмкіндігіне алып келеді.

Бірінші қауіп-физикалық шабуыл. Ақпараттың таралуының ең қарапайым себебі бұл ақпарат орналасқан компьютерге физикалық қол жеткізу мүмкіндігі болып табылады. Физикалық қауіпсіздік компьютерлік жабдықтарды оған физикалық қол жеткізуді шектеу арқылы қорғауды білдіреді. Компьютер немесе басқа құрылғы ұрлығы 2011 жылдың екінші жарты жылдығында ақпараттың барлық жайылып кетуінің 57%-ы және бірінші жарты жылдықта 46%-ы себеп болды.

Екінші қауіп – әлеуметтік шабуылдар. Компьютерлік шабуылдаушыларға парольмен қорғалған жүйелерге енудің ең тиімді әдістерінің бірі құпия сөзді сұрайтын техникалық қолдау қызметі арқылы пайдаланушылардан құпия мәліметтерді алу.

Бірақ көбінесе желіге қол жеткізу үшін әлеуметтік инженерия әдісі қолданылады оған көп көңіл бөлінбейді. Әлеуметтік инженерия (ағылш. social engineering) адамның мақсатына жету үшін жеке басын басқаруға негізделген.

Қауіпсіздік қызметтері антивирустар орнатып, төзімділік пен парольдердің күрделі жүйесін әзірлеп жатқанда, шабуылдаушылар қарапайым ештеңе сезбейтін пайдаланушыларды пайдаланып желіге енеді.

Шын мәнінде, шамамен 70%-ы бұзу мен компьютерлік жүйелерге ену әлеуметтік инженерия арқылы жүзеге асады. Бұл бағыт өте маңызды, сондықтан адамдар оны компьютерлік жүйелерді оқудан гөрі оны зерттеуге көп уақыт бөлуі керек [1].

Ақпараттық қауіпсіздіктің кез келген құрылымындағы ең әлсіз буын адам болып табылатынына назар аударғым келеді. Сенімді қорғау жүйесін құруға және қауіпсіздік бойынша өте егжей-тегжейлі нұсқаулықтар жазуға болады, алайда қызметкерлердің маңызды мәліметтермен немқұрайлы қарауы, олардың сенімсіздігі мен бейқам мінез-құлқы барлық күш-жігерді жоққа шығаруға қабілетті.

Бұл тәсіл әлеуметтік-психологиялық модельдеуді қолдана отырып, технологиялық жаңашылдықты, есептеулердің инженерлік дәлдігін біріктіруге мүмкіндік беретін әдіснамалық және талдауды қолдайтын жүйелік тәсілге негізделген. Бұл құралдарды игеру әлеуметтік инженерлер үшін «өз еркімен» және «өз бетінше» әрекет ететін адамдардың мінез-құлық моделін табысты құрудың кепілі.

Әлеуметтік инженерия дегеніміз - техникалық құралдарды пайдаланбай ақпаратқа немесе ақпаратты сақтау жүйесіне рұқсатсыз қол жеткізу әдісі. Әлеуметтік инженерлердің басты мақсаты кез-келген деректерді ұрлау үшін қауіпсіз жүйелерге қол жеткізу болып табылады. Қарапайым бұзушылықтың басты айырмашылығы - бұл машина емес, шабуылдың нысаны ретінде таңдалған оның операторы. Сондықтан әлеуметтік инженерлердің барлық әдістері мен техникасы адам факторының әлсіздігін пайдалануға негізделеді, бұл өте жойқын деп саналуы мүмкін, өйткені қаскүнем ақпаратты, мысалы, телефон арқылы немесе ұйымға оның қызметкері ретінде кіру арқылы алады.

Осындай шабуылдардан қорғану үшін сіз қаскүнемнің кең таралған түрлерінен хабардар болуыңыз керек, сіз әлеуметтік инженерлердің нені қалайтынын түсініп, тиісті қауіпсіздік саясатын уақтылы ұйымдастырыңыз. Бұл әлемдегі барлық ақпаратты адамдар қорғайды, оның негізгі тасымалдаушылары сонымен қатар әдеттегі жиынтықтары, әлсіздіктері мен болжамдары бар адамдар болып табылады, олардың көмегімен әлеуметтік инженерлер қалаған деректерге қол жеткізеді. Бұл жұмыс мұны қалай жасауға және одан қорғану амалдарын әзерлеуге арналған.

Бағдарламаның бұзылу себептері мен әдістерін және әртүрлі құрылымдардан ақпараттың ағып кету арналарын талдай отырып, біз шамамен 80% жағдайда себеп адам факторы немесе оны басқару деген қорытынды жасай аламыз.

Ғылыми жұмыстың өзектілігіне жоғарыдағы айтылған ақпараттар негіз бола алады.

Жұмыстың мақсаты: әлеуметтік инженерияның зардап шеккен адамға әсер ету әдістерін сараптай келе, осалдықтарға қарсы іс-қимыл әдістемесін әзірлеу.

Осы мақсатқа жету үшін келесі міндеттер қойылды және шешілді:

- әлеуметтік инжирингпен байланысты қауіптерді және әлеуметтік инженерлер пайдаланатын негізгі қолданыстағы әдістерді анықтау;
- әлеуметтік инжинирингке қарсы іс-қимылдың негізгі тәсілдерін сипаттау;
- әлеуметтік инжинирингке қарсы іс-қимыл әдістемесін әзірлеу.

Жұмыстың ғылыми жаңалығы ақпараттың «әлеуметтік инженерия» сияқты шабуылдардан қорғалуын қамтамасыз ету әдістерін әзірлеуде жатыр. Бұл тәсілдер ұйымның өмір бойы қорғалуын арттыруға мүмкіндік береді.

1 Әлеуметтік инженерия

1.1 Әлеуметтік инженерияның өзектілігі

Қазіргі кезде ақпарат ең құнды және ең құпиялы құбылыстардың бірі болып табылады. Қазіргі кезде ақпараттар әр түрлі мақсатта қолданылуы мүмкін. Мысалы, ақпаратты сатуға, өз игілігіне қолдануға немесе ақпарат арқылы біреуді бопсалауға, мәжбүрлеуге және тағы да басқа әрекеттерде қолданылуы мүмкін. Үстіде келтірілген себептерге сай қазіргі таңда ақпараттың құны өсуде. Ақпараттың құны өскен сайын, оны қолына түсіргісі келетін адамдар саны геометриялық прогрессияда өсуде. Ақпарат әр- түрлі күйде бола алады (параққа жазылған сөздер, дауыс, электронды түрде және т.б.). Ақпараттың келбеті, түрі көп болғанына байланысты, зиянкестер ақпаратты заңсыз жолмен қолына жеткізу үшін сәйкесінше әр түрлі амалдарды қолдануда. Бұл амалдардың ішінде әлеуметтік инженерияда бар.

Ғылыми жұмыстың тақырыбын әлеуметтік инженерия болып таңдалу себебі, қазіргі кезде әлеуметтік инженерия өте өзекті мәселелердің бірі болып табылады. Бұған дәлел осы жылдағы әлеуметтік инженерияға тап болған зардап шегушілер саны 65%-ға өсті. Зардап шегушілер қатарында жеке тұлғалар, кіші орта және ірі кәсіпорындар бар. Әлеуметтік инженерия ұғымы шыққан кезден бастап бұл ұғым бір мезетке де өз өзектілігін жоғалтқан жоқ, керісінше өзінің өзектілігін ұлғайтуда. Бұл өзектілік ұлғайған сайын, әлеуметтік инженерияны заңсыз жолмен қолданғысы келетін адамдар саны ұлғайып жатыр. Қазіргі кезде ақпараттың ұрлануының 70%-ы әлеуметтік инженерия арқылы жүзеге асырылады. Бұл пайыздарға дәлел соңғы кезде үлкен және орта корпорацияларға жасалған 20 шабулдардың 12-сі әлеуметтік инженерия арқылы жасалған, бұл 70%-дан астамы. Ал корпорацияларды ғана емес, барлық шабуылдарға келетін болсақ бұл пайыз 90-ға жетеді. Әлеуметтік инженерияның қарқынды даму себебі, барлық жүйеде ең осал ол техника емес, адам болып табылады. Қазіргі таңда әлеуметтік инженерия арқылы жасаған шабуылдардан зардап шегушілер шамамен 25 000-100 000 доллар арасында қаражат жоғалтады. Компания әлемдегі ақшаға сатып алуға мүмкін ең үздік қорғану жүйелерін сатып алатын болса да, жұмыскерлерін жұмыс орнынан шыққан сайын құпия ақпаратты тығып кетуге үйретсе де, әлемдегі ең үздік күзет орындарынан күзетшілерді жалдайтын болса да, бұл компания толығымен осал болып келеді. Жұмыскерлер, эксперттер кеңес берген ақпараттық қауіпсіздіктің ең үздік ережелерімен жүрсе де, жаңа шыққан ережелерді мүлк етпей орындаса да толығымен осал болып есептеледі [2].

Бұған дәлел Ресей мемлекетінде 2018 жылы банктерден, орта және үлкен компаниялардан шамамен 750 млн. руб. әлеуметтік инженерия арқылы ұрланған. Банктердің қауіпсіздігі үздік технологиялармен қорғалады. Бірақ бұл

технологиялар адамның мінез құлық, әдеттерінін осалдылығына қарсы тұра алмайды. Сондықтан тек технологияларды күшейтумен тоқтап қалмай, жұмыскерлердің шеберліктерін күшейту керек.

1.2 Әлеуметтік инженерияның пайда болу уақыты, тарихы

Әлеуметтік инженерия тұралы ең алғашқы рет 70-ші жылдардың басында естіле бастады. Ол кездері жүйелер өте қарапайым болған. Қарапайым болғанның өзінде жүйелер тек ірі корпорацияларда болған. Осы кезде компьютерлік технологияларда әлеуметтік инженерия түсінігі пайда болды. Бұл уақытта әлі компьютерлік жүйелер болмаған, бірақ телефонды жүйелер болған. Ал жүйе бар жерде хакерлер бар, нақтылай айтсам фрикерлер.

Фрикерлердің ең алғашқы қызуғушылықтарының бірі, операторларға қоңырау шалып олардың құзыреттіліктері туралы сөйлесіп, мазақ қылу. Операторлар, әсіресе жаңа жұмыскерлерден олар таныс емес ақпарат сұраған кезде, жұмыскерлер ақтала бастайтын. Біраз уақыт өткеннен кейін, зиянкестер бұл әдісті тек қызықшылық мақсатында емес, ақпаратты заңсыз жолмен алу мақсатында қолданған. 70-ші жылдардың соңына таман әлеуметтік инженерияның бұл әдісі дамығаны соңшалықты, тәжірибелі фрикер жұмыскерден өзіне керек ақпараттың бәрін алып қолданатын.

Келесі қадамда компьютерлік жүйелер пайда болды. Бұрында фрикерлер операторлардың құлақтарына отырып, сол арқылы керек ақпаратты алатын. Ал қазіргі кезде бір құпия сөз арқылы бүкіл ақпаратты алу мүмкіндігі пайда болды.

Фрикинге мысал келтірсек, 1970 жылдары Кевин Митниктің алдын ала дайындықтан өткен фрикингтік қоңырауларын атап көрсетуге болады. Кевин Митник телефонын келесі жағында отырған жұмыскерге сенімді болып көрінуі үшін, компанияның әр түрлі бөлімшелерін зерттеп ақпарат жинаған. Ақпаратты оңтайлы уақытта қолданып, өзіне керек ақпаратты алған. Бұл фркинигпен тоқтап қалмай авторизациялаудан өтпеген телефонды коммутаторды бұзу алаяқтығымен айналысқан. Яғни, телефондардың мекен жайларын ауыстырып шатасытыратын.

Әлеуметтік инженерия адамзатқа таныс болмай тұрып, қолданыста ие болатын. Оған дәлел, 1960 жылы Фрэнк Абанналэ Pan Am компаниясының жұмыскерлерін және басқа адамдарды өзі комерциялық ұшқыш екеніне сендірді. Фрэнк Абанналэ мектеп журналисті ретінде компанияның саясатын, процедураларын және өнеркәсіптің бағаланбас терминологияларын біліп алды. Алған ақпаратын және Pan Am ұшқыштарының киімін қолдана отырып әлем бойынша тегін ұшатын. Тегін ұшумен шектелмей, банктік үрдістер тұралы ақпаратты қолданып Pan Am компаниясының чектері арқылы ақша ұрлайтын [3].

Демек әлеуметтік инженерия 1970 жылдардың басында естілгенімен, бірақ сол уақытқа дейін қолданыста болған. Әлеуметтік инженерия 1970 жылдардан бастап, қазіргі таңда да актуалді мәселе болып табылады. Үстіде келтірілген

фактілерге сүйене отырып, әлеуметтік инженерия болашақтада актуальді мәселе болып қала беретіндігіне күмән келтіруге негіз жоқ. Себебі, адамзат қаншалықты дамығанымен машина емес, адамдардың эмоцияларымен, мінез құлқымен оңтайлы уақытта дұрыс қолдана білсең қызықтыратын ақпаратты алу мүмкін болып табылады. Ал оған орай электронды құрылғылармен қолдана білу бұл ықтималдылықты 100%-ға көтереді.

Әлеуметтік инженерия дегеніміз - социология, психология және алаяқтық әдістерді қолдану арқылы, ақпараттың негізгі қасиеттерін (конфиденциалдылығын (құпияланғандық), тұтастығын, қатынау қолайлығығың) бұзу арқылы қалаған мақсатына жету амалы. Әлеуметтік инженердің мақсаты - адам туралы жасырын ақпаратты немесе пайда алып келетін құпия ақпараттарды алаяқтық жолмен алу. Құпия ақпарат - бұл логин/ құпия сөз, жеке деректер, банк карталарының нөмірлері және қаржылық немесе беделді шығындарға алып келетін барлық нәрсе [4].

Көбінесе әлеуметтік инженерияны ақпаратқа заңсыз қол жеткізу амалы деп ойлайды, бірақ бұл толығымен шындық емес. Әлеуметтік инженерияны кей жағдайларда заңды түрде қолданады. Мысалы, қол жетімсіз нәтижелерге қол жеткізу немесе оң істерге алып келетін жағдайға адамдарды және топтарды програмаллау үшін қолданылады. Әрине қазіргі кезде әлеуметтік инженерияны көбінесе ғаламтор желісі арқылы құнды ақпараттарға қол жеткізу үшін қолданады, бірақ қазіргі замандық әлеуметтік инженерлер, әлеуметтік инженерияны жеке бизнесін үлкейту және нәтижелерін нығайту үшін қолданады. Бұған дәлел, әлемге есімдері әйгілі әлеуметтік инженерлер Дэвид Бэннон мен Питер Фостер өздерінін кіші кәсіпорындарын дамыту мақсатында әлеуметтік инженерияны қолданған.

Әлемге есімдері әйгілі шабуылдаушы-инженерлер:

- Кевин Митник. Әлемдегі ең әйгілі қоғамдық инженерлердің бірі болып Кевин Митник саналады. Әлемге атты әйгілі хакер және қоғамдық инженер бола тұра, Митник көптеген компьютерлік қауіпсіздік тақырыбындағы, әсіресе қоғамдық инженерияға көңіл бөлетін кітаптардың авторы. 2001 жылы «Исскуство обмана» атты Митниктің кітабы дүиеге келді. «Исскуство обмана» кітабында қоғамдық инженерияны шанайы өмірде қолданғаны тұралы жазылған. Кевин Митниктің айтуы бойынша құпия сөзді өтірік айту арқылы алу, компьютерді бұзу арқылы алғаннан оңай. Кевин Митник адал жолға түскен уақыттан бері әлеуметтік инженерия туралы бірнеше кітап жазған. Оларға мысалы, «Исскуство обмана», «Исскуство вторжения», «Призрак в проводах» және т.б.
- Ағайынды Бадирлар. Бұл екі ағайынды Мушид және Шадир Бадир туыла соқыр болғанымен, әлемге танымал қоғамдық инженерлер болып табылады. Ағайынды Бадирлар 1990 жылы Израильде алаяқтықтың бірнеше ірі схемаларын құрып, оларды жүзеге асырған. Интервью кезінде ағайынды Бадирлардың айтуы

бойынша, жүйелік шабуылдардан тек қана телефон, ноутбук немесе басқа электронды құралдарды қолданбайтын адам ғана толық қорғанған. Ағайындылар ұялы телефондар жүйелерінің интерференциалды тондарын естіген үшін абақтыда отырған. Олар шет елге ұзақ уақыт бойы қоңырауды тегін шалып жүрген.

- Архангель. Архангель әйгілі компьютерлік хакер және ағылшын тіліндегі Phrack Magazine атты журналдың қауіпсіздік консультанты. Архангель қоғамдық инженерияның әдістерін көрсетіп, бірнеше жүздеген адамдарды алдаған.
- Басқа әлеуметтік инженерлер. Аттары танымал Фрэнк Абигнейл, Дэвид Бэннон, Питер Фостер және Стивен Джей Рассел атты қоғамдық инженрлер бар.

Жоғарыда жазылған әлемге есімдері әйгілі әлеуметтік инженерлердің өмірбаяндарын, берген кеңестерін оқи отырып әлеуметтік инженерия қазіргі таңда, шыққан кезінен бастап өз актуалдылығын жоғалтпағанын көрдім. Әйгілі әлеуметтік инженерлердің қолданған амалдарын зерттей келе, әлеуметтік инженерияны тек зиян жағынан емес, өз ісінді өркендету мақсатында қолдануға мүмкін екенін көруге болады [3].

2 Әлеуметтік инженерия әдістері

Әлеуметтік инженерияның барлық әдістері когнитивті бұрмалануларға негізделген. Бұл мінез-құлық қателіктерін, әлеуметтік инженерлер тарапынан жасырын ақпаратты алуға бағытталған шабуыл жасау үшін пайдаланады, көбінесе жәбірленушінің келісімімен. Адамдардың эмоцияларының және мінез құлықтарының осалдылығын әлеуметтік инженерлер біліп, осалдылықтармен толыққанды қолданады.

Мысалы, компанияға бейтаныс адам кіріп, хабарландыру тақтасына, ресми тұрғыда жасалғанға өте ұқсас хабарландыру іледі. Хабарландыруда ғаламтор желісінің провайдерінің ұялы телефон нөмірі ауысқандығы тұралы ақпарат жазылған. Компания қызметкерлері хабарландырудағы нөмірге қоңырау шалған кезде, зиянкес өзін ғаламтор желісінің провайдері ретінде таныстырып, құпия ақпаратты алу үшін жұмыскердің логиндері мен құпия сөздерін сұрауы арқылы компанияға тиесілі құпия ақпараттарды заңсыз жолмен алуы мүмкін.

Үстіде келтірілген мысалға сүйене отырып, адамның немесе қоғамдық топтардың когнитивті бұрмалануына бір ғана хабарландыру жеткілікті екенін байқауға болады. Бұл адамзаттың осалдылығын білдіреді.

Әлеуметтік инженерияның бірнеше амалдары бар. Бұл әдістер төмендегі тізімде көрсетілген:

- претекстинг;
- фишинг;
- Кво туралы кви;
- жолдағы алма;
- ақпараттарды ашық көздерден іздеу;
- трояндық вирус әдістері.

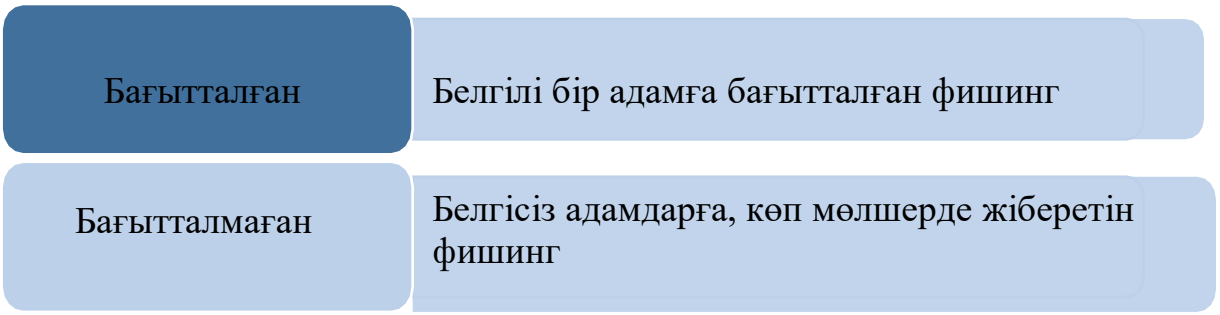
Бұл амалдарды қолдану үшін, зиянкесте алдымен зардап шегуші тұралы бастапқы ақпараттар болуы керек (аты жөні , атқаратын қызметі, жасап жатқан жобасының атауы, туылған жылы, күні туралы ақпарат). Кішігірім мысал ретінде, зиянкес алдымен шынайы жобаға байланысты сұрақтарын қойып, сеніміне кіргеннен кейін, оған өзін қызықтыратын құпия ақпараттарды біліп алу нәтижесінде сұрақтар қояды [5].

2.1 Фишинг

Фишинг – ғаламтор желісіндегі алаяқтық болып табылады. Фишингтің басты мақсаты, әртүрлі жүйелерде авторизацияланған пайдаланушылардың құпия деректерін ұрлау болып табылады (логин, пароль, карталардың нөмірлері және тағыда басқа). Фишингтік шабуылдың басты әдісі болып, поштаға жалған хабарламаның келуі болып табылады. Келген хат ресми компанияның хатына немесе банктің ресми хатына ұқсас болып келеді. Ол хатта деректерді еңгізуге

болатын бағандар немесе деректерді еңгізуге болатын бағандары бар web парақшасының сілтемесі болады. Бірақ қазіргі таңда әлеуметтік желілердің дамығанымен қатар фишиингтік хабарландыруларды жіберу аланы өсуде. Пайдаланушылардың бұндай алаяқтыққа алдану себептері әр- түрлі бола алады. Мысалы, деректердің жоғалуы немесе жүйелердің бұзылуы т.б.

Фишингтік шабуылдар екіге бөлінеді:



3.1 сурет – Фишинг шабуыл түрлері

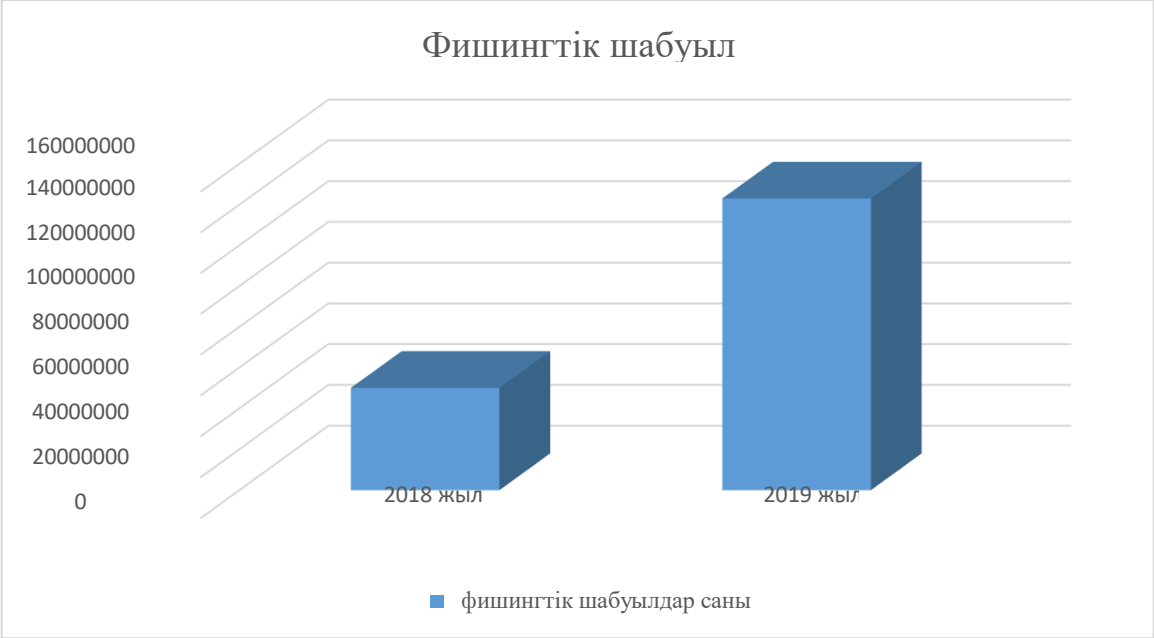
Бағытталған фишингтік шабуыл белгілі бір адамға жасалады. Фишингтің бұл түрі жүзеге асуы үшін зардап шегушіні толығымен зерттеу қажет. Зардап шегушінің қызығушылығы қандай, ұялы телефон маркасын, отыратын әлеуметтік жүйелері және т.б. Осы ақпараттарды қолдана отырып бағытталған шабуыл жасаған кезде, шабуылдың жүзеге асу ықтималдылығы жоғары болады.

Бағытталған фишингтік шабуылға мысал келтіретін болсам 2016 жылы болған «4127» атты топ Хиллари Клинтонның президенттік компаниясының мүшелеріне бағытталған фишингтік шабуыл жасалуы. Зиянкестер 1800 google электронды поштасына шабуыл жасап accounts-google.com доменін берген және пайдаланушыларды бопсалаған.

Бағытталмаған фишингтік шабуыл әдісінде фишингтік сілтемелер ірі, аттары әлемге әйгілі компаниялар атынан келеді. Бұл ауқымды фишингтік шабуылдар белгісіз көптеген пайдаланушыларға жіберіледі. Аты айтып тұрғандай фишинг балық аулауға ұқсас келеді. Фишингке біреу түседі, біреу түспейді. Сондықтан, фишингтің бағытталмаған түрі көп кездеседі.

Зерттеулердің көрсетуі бойынша 2018 жылы әлем бойынша компаниялардың 85 пайызына фишингтік шабуылдар жасалған. Бұл алдынғы жылмен салыстырғанда 65 пайызға көп.

Астыда көрсетілген диаграммада көрсетілгендей 2017 жылы шамамен 50000000 фишингтік хаттар жіберілген болса 2018 жылы шамамен 143000000 фишингтік хабарландырулар жіберілген [6].



3.2 сурет – Фишингтік шабуылдардың 2018-2019 жылдағы көрсеткіші

CyberEdge компаниясының зертеулері бойынша 2017 жылы жасалған фишингтік шабуылдардың 71% жүзеге асты ал, 2018 жылы 76% көрсетті. Бұл көрсеткіш 2019 жылы 79% көтерілді.

Әлемге әйгілі фишингтік амалдар:

- әлемге әйгілі компаниялар брендттерінің есімдерін қолдану;
- жасанды (өтірік) лоторея;
- жалған антивирустар мен жалған қорғау бағдарламаларын қолдану;
- телефон арқылы жасалатын фишинг (вишинг);
- жоқ сілтемелерді жіберу.

1. Әлемге әйгілі компаниялар брендттерінің есімдерін қолдану әдісі – бұл әдісте поштаға келген хат, әйгілі компаниялардан келген хабарландыру секілді келеді. Келген хабарландыруда сілтемелер болуы мүмкін. Сілтеме батырмасына басқан кезде, көз алдымызда компанияның ресми web парақшасына максималды ұқсас парақша ашылады. Хабарландыруда компания өткізген конкурстан жеңімпаз атандыңыз деген хабарлама немесе сіздің парақшаңыздың деректерін шұғыл түрде ауыстыру керек деген хаттар келуі мүмкін. Бұндай алаяқтықтар телефон арқылы да жүзеге асырыла алады.

2. Жасанды лоторея әдісі – бұл әдісте пайдаланушыға сіз конкурстан ұттыңыз деген хабарландыру келеді. Пайдаданушылардың алдану себебі, хат әлемге аты әйгілі компанияларға ұқсас фишингтік парақшадан келеді.

3. Жалған антивирустар мен жалған қорғау бағдарламаларын қолдану әдісі – бұндай алаяқтық бағдарламалар “scareware” деген есіммен белгілі. Бұл

бағдарламалар антивирус секіліді көрінеді, бірақ атқару қызметі мүлдем керісінше. Scareware, пайдаланушыға әртүрлі қауіптерді жалған түрде генерациялап жібереді және алаяқтық транзакцияларға бұрмалайды. Пайдаланушылар бұл жағдайға электронды пошта, онлайн хабарламалар, социалді желілер, қалқымалы терезеден шығатын хабарландырулар арқылы соқтығысуы мүмкін.

4. Телефон арқылы жасалатын фишинг (Вишинг) бұлай аталуы себебі, фишингке ұқсас болып келеді. Фишингтің бір түрі деп айтса да болады. Бұл әдіс, алдын ала жазылып алынған дауыстар арқылы жасалады, сонда пайдаланушы бұл хабарлаушыны банктің немесе қалған IVR жүйелерінің ресми тұлғасы деп ойлайды. Әдетте пайдаланушыға фишинг парақшасы электронды поштаға келеді. Хатта пайдаланушы өзінің деректерін банк жұмыскеріне хабарласып өзгертуі керек немесе оны расстау керек деген хабарландыру келеді. Пйдаланушы жүйеге кіру үшін, пайдаланушыдан аутентификациядан өтуін талап етеді. Аутентификация PIN -ты және парольді енгізу арқылы жүзеге асырылады. Сондықтан алдын- ала жазылған жазба арқылы көптеген өзіне керек ақпаратты біліп алуға болады. Мысалға, әр адам алдын ала (құпия сөзіңізді өзгерту үшін 1 басыңыз, оператордың жауабын алу үшін 2-ні басыңыз) деген жазбаларды жазу мүмкін. Жазбаларды уақытысында қосып, автоматты түрде айтылатын сөздер ретінде көрсетуі мүмкін.

5. Жоқ сілтемелерді жіберу әдісі – келесі жолмен орындалады. Пайдаланушыға хабарландыру келеді. Хат жіберген зиянкестің есімі, пайдаланушыны қызықтыратындай болады. Хат ішіндегі сілтеме пайдаланушыны азғыртатындай болып келеді. Мысалы, “PayPal” денген сілтеме келеді,сілтеме “PayPal” ресми парақшасына ұқсас болып табылады, бірақ әр пайдаланушы бұл алаяқтықты байқамайды. Бұл әдіске мысалы 2003 жылы болған оқиғаны келтірсек болады. 2003 жылы мыңдаған ebay пайдаланушыларына фишнгтік хат келеді. Хабарландыруда, пайдаланушылардың парақшалары бұзылғандығын жазады. Парқашаны қалыпты күйіне келтіру үшін, пайдаланушыларға карталарының деректерін қайта енгізуді талап еткен. Эксперттердің зерттеулері бойынша, сол шабуылдан кейін пайдаланушылар жалпы есеппен бірнеше миллион доллар көлеміндегі шығындарға тап болған.

Қазіргі кезде ақпаратты қорғау алдыға нық қадам жасады. Сонымен қоса, іздеу жүйелерінің әзірлеушілері де сәйкесінше қадамдар жасауда. Сондықтан, қазіргі кездегі жүйелердің көбісі фишингтік хаттарды және зиянкес парақшаларды анықтай алады. Анықталған хаттарды спамға салады. Антивирустар одан да жақсы қорғайды. Бірақ өкінішке орай, даму деген екі жақты құбылыс. Қорғаныс күшейген сайын, зиянкестерде әр түрлі жолдар ойлап табуда. Сондықтан, фишингтік шабуылдар әлі күнге дейін актуалды болып

табылады, себебі хабарламалар және web парақшалар зиянкестің ойлаған уақытына сай қолданылса пайдаланушылардың алдануы әбден мүмкін.

Фишингке жасалған практикалық жұмыс. Алдымен фишингке айналатын ресми парақша таңдалады. Қазіргі кезде дүние жүзінің 2,5 млрд адамы қоғамдық жүйелерде отырады. Соның ішінде ВК қоғамдық жүйесінде айына 97 млн адам отырады. Қазақстанның өзінде ВК әлеуметтік жүйесіне 2 миллион активті падаланушы тіркелген. Үстіде келтірілген фактілерге сүйене отырып ВК қоғамдық жүйесі таңдалған. Келесі қадамда ВК қоғамдық жүйесін толығымен зерттеу жүргізіледі. Күй келбетін, доменін және т.б.

Келесі қадамда SmartApe хостинг парақшасына тіркелу процесі орындалады. SmartApe хостингтік парақшаны тандау себебі - 14 күн тегін қолдануға болады. FTP пайдаланушысы статусы таңдалады. Ninite бағдарламаларды таратушы сайтынан Fille Zilla бағдарламасы орнатылған. Fille Zilla бағдарламасы тегін ашық FTP клиенттік бағдарлама болып табылады. Fille Zilla бағдарламасына хостинг парақшасындағы идентификациялау деректері енгізіледі. Хост адресін жазып, клиенттік бағдарламаға өз атымен кіру керек. Домендердің папкасына кіріп ВК парақшасының пішінінің скрипттерін Fille Zilla-ға (серверге) орнату қажет. Түсінікті болу үшін Fille Zilla ол SmartApe парақшасымен байланысты. Енді вк-нің фишингтік парақшасы пайда болды. Оны хостинг парақшасы арқылы кіріп қарауға болады. Бірақ дегенмен фишингтің парақшасының сілтемесі, ресми вк парақшасынан мүлдем өзгеше. Бұл ақаулықты өзгерту мақсатында Freenom.com парақшасына кіріп фишингтік парақшанын сілтемесін vk01.ga ауыстыру керек.

Енді вк қоғамдық жүйесінде авторизацияланған адамдардың ішінен кез келген адамды таңдаймыз. Таныс достарының біреуін таңдау дұрыс болып саналады. Себебі, таныс адамды зерттеуге уақыт кетірмейсің. Таныс емес адамға жіберуге болады. Бірақ бөтен адамға жіберсең, біріншіден ол адам немен қызығатынын білу керек. Екіншіден, ол адамның жеке құқығын бұзу деп саналады. Сондықтан, әрине бөтен адамға жіберген дұрыс. Алдымен пайдаланушы немен қызығатының біліп алу керек. Пайдаланушы корей елімен толығымен қызығатыны белгілі болды. Корей тағамымен, корей киімдерімен, корей адамдарының түр келбеттерімен қызығатыны анықталды. Сондай-ақ, Корей қыздарының түр келбеттеріне еліктейтіні белгілі болды. Логикалық тұрғыдан ойлап қарасақ, корейлердің түр келбетіне еліктесе, яғни корейлер секілді болғысы келеді деген сөз. Ондай жағдайда өзіне қарап жүреді. Өзіне қарайтын адам болса, өзі тұралы адамдар не ойлайтынына қарайды.

Келесі қадамда, вк қоғамдық желісінің ресми парақшасына максималды ұқсас фишингтік парақша құрылады. Доменнің ресми түріне ұқсас доменге ауыстыру процесі орындалады. Енді, құрылған фишингтік парақшасының сілтемесі жәбірленушіге жіберіледі. Фишигтік парақшаға өзінің деректерін енгізді. Деректермен кез келген заттар жасауға болады. Деректерді қолданып

құпия ақпараттарды алуға, ақша талап етуге және т.б. алаяқтық іс-әрекеттер жасауға болады.

Фишингке жасаған зертеу жұмысымызда талдаймыз:

- алдымен, фишинг жасалынатын аумақты таңдалады;
- фишингке алданатын пайдаланушыларды таңдау жүзеге асырылады;
- пайдаланушылар туралы мәліметтер жинақталып, зерттеледі.

Бүкіл ақпаратты қолдана отырып, фишингтік парақшаны жүзеге асыру орындалады. Зардап шегушіге электронды пошта арқылы хабарландыру жіберіледі.

Адамдарды фишингтік парақшаларды айқындауға және фишингпен әр түрлі әдістермен қарсы тұруға үйретуге болады. Көптеген ірі компаниялар жұмыскерлердің шеберліктерін білу мақсатында симуляциялық фишингтік шабуылдар жүргізеді.

Фишингке қарсы қолданатын амалдар ұсыну:

- Сайттың жеке дизайны. Бұл әдістің мәні пайдаланушы сайтқа кірген кезде сайттың фонын өзі таңдайды. Келесі реттерде кірген кезде сайт пайдаланушы таңдаған фонмен қосылады. Егер пайдаланушы сайтқа кірген кезде, фонды көрмесе немесе басқа фонды көрсе ол жалған сайттан дереу мезетте шығып, қауіпсіздік қызметтеріне хабарласу керек. Болжам бойынша зиянкес, зардап шегуші фонды таңдаған кезінде қасында болмаса, пайдаланушы таңдаған фонды біле алмайды.
- Бір реттік құпия сөздер. Яғни қазіргі кезде, көптеген адамдар бір құпия сөзді бірнеше банктік карталарға қолданады. Бұндай құпия сөздерді зиянкестер біліп алатын жағдайда, зиянкес құпия сөзді өзі қалаған уақытында бірнеше рет қолдана алады. Ал бір реттік пароль кезінде, бір парольді бірнеше картаға емес, бір карта үшін әр түрлі құпия сөздерді қолданады. Яғни, пайдаланушы жаңадан кірген сайын жаңа құпия сөз енгізіп тұрады. Қорғанудың бұл әдісі сандар генераторлары арқылы жүзеге асырылады. Сандар генераторы әр түрлі құпия сөздерді бес он минут сайын өзгертіп тұрады. Пайдаланушы картаны енгізген кезде, өзінің генераторын іске қосып, генератордағы құпия сөзді енгізеді. Қазіргі кезде генераторлар әр түрлі пішімді, сондықтан ыңғайлылықпен мәселе туындамайды. Яғни ыңғайлы және ең бастысы қауіпсіз.

2.2 Претекстинг

Претекстинг бұл алдын ала ойластырылған, тәжірбиеленген әрекеттер жиынтығы. Нәтижесінде зардап шегуші кейбір ақпараттарды беруі мүмкін немесе зиянкес айтқан әрекеттерді жасауы мүмкін. Претекстинг әдісін қолдану алдында, зиянкесте зардап шегуші тұралы ақпараттар болуы тиіс. Қолдағы ақпараттар арқылы зиянкес өзінің шын жүзін зардап шегушіден жасырын ұстап қала алады.

Көбінесе бұл шабуыл түрі аудиожазбалар арқылы немесе Skype секілді әлеуметтік желілер арқылы жүзеге асырылады.

Бұл амалды қодану үшін, зиянкесте алдымен зардап шегушінің ақпараты болуы керек (аты жөнін, атқаратын қызметін, жасап жатқан жобасының атын, туылған жылы күні туралы ақпарат). Зиянкес алдымен шынайы жобаға байланысты сұрақтарын қойып, сеніміне кіргеннен кейін, оған өзін қызықтыратын құпия ақпараттарды біліп алу нәтижесінде сұрақтар қояды [7].

Претекстингке мысал, зиянкес зардап шегушіден белгілі бір соммадағы ақша алғысы келіп тұр. Қазіргі кезде адамның телефонын немесе қоғамдық жүйедегі парақшасын тауып алу оңай. Зиянкес зардап шегушінің парақшасын және телефон нөмірін тауып алды. Ғаламтор желісінде адам туралы жүз пайыз ақпарат болмаса да, басты ақпараттар бар. Осы басты ақпаратты қолдана білетін әлеуметтік инженер өзіне қалаған ақпаратты немесе ақшаны қолына түсіре алады. Бұл ақпараттарға ұялы телефон нөмері, тұратын мекен жайы, жұмыс орны және тағы да басқа ақпараттар кіреді. Зиянкес ғаламтор желісі арқылы зардап шегушінің туған ағасы бар екенін тапты. Ағасының қоғамдық желідегі парақшасын тауып зерттеп, сол адам секілді ойлауға тырысады. Зардап шегушінің әлеуметтік желідегі парақшасын бұзып ағасы екеуінің хабарламаларын оқиды. Зиянкес зардап шегушіні хабарламалар арқылы зерттейді, зардап шегуші тұралы фактілерді тауып алады. Оған зардап шегушінің лақап аты, ортақ таныстарының есімдері, бірге баратын орындарының аттары және тағы да басқа. Осы жинаған ақпарат бойынша зиянкес жоспар құрады. Бұл жоспарда, зиянкес зардап шегушінің ағасының атынан түн ортасында хабарласып, біреу оны ұрып, ұялы телефоны мен ақша құжаттарын ұрлап алып кетті деп айтады. Бұл сөздерден кейін неге басқа нөмірден хабарласып тұрсын деген сұрақтар қойылмайды. Маңызды сәттердің бірі, зиянкес зардап шегушіге есімі арқылы емес, лақап атымен сәлемдесті. Зардап шегушінің лақап атын ағасы екеуінің хабарламаларынан біліп алды. Келесі қадамда зиянкес екеуіне ортақ таныс адамдардың есімдерін айтып, сол адамдармен бірге болғанын айтады. Бірақ ата аналарына айтпауын сұрайды, себебі атасының жүрегі ауыратынын ескертеді. Барлық ақпаратты хабарламалардан біліп алды. Осындай фактілерден кейін, сеніп қалған зардап шегушіден зиянкес таксиге ақша сұрайды және карточканың нөмерін береді. Карточка иесі хабарласуға ұялы телефонын берген адам деп айтады. Бұндай жасалған әрекеттерден кейін он адамның сегізі алданады [8].

Претекстинг тәсілі шабуылдаушы бойынша қолданылған іс-шаралар:

- өзіне керек адамның рөлін (ағасының) және сенімді оқиға ойлап тапты. Оқиғаны шынайы фактілермен толтырды (атасы туралы ақпарат, таныс адамдары тұралы ақпарат және лақап аты т.б.);
- барлық оқиға тез уақытта айтылды. Әлеуметтік инженерлердің басты ережелерінің бірі, адамға ойлануға мұрша бермей, оны жұмыс істету. Бұл

психологиялық әдіс назарды қадағалап ұстай білу әдісі деп аталады;

- ең маңызды механизмдердің бірі қолданылды. Жаңашырлыққа қысым жасалды. Бұл қысым зардап шегушінің ағасы болғандықтан өрши түсті;

- бұл оқиға өте оңай және сенгісіз көрінгенімен бұндай әдіске көптеген зардап шегушілер алданады. Себебі, адамның эмоциялары және мінез-құлқының осалдалығы өз рөлін ойнайды. Бұған дәлел ретінде дипломдық жоба барысында жасалған мысалды алуға болады. Осылайша жоғарыда келтірілген оқиғаға ұқсас зерттеу жүргізіледі.

Претекстинке жасалынған мысал: алдымен зардап шегушіні таңдалады. Зардап шегуші ретінде Асхат есімді жігіт таңдалды. Әлеуметтік желілер арқылы туылған жылын, instagram желісін тауып, әлеуметтік желідегі достары арқылы электронды поштасының адресі анықталды.

Электронды поштасына үстіде жасалған ВК әлеуметтік желісінің фишингтік парақшасынын сілтемесін жіберілді. Сенімді көріну үшін ВК әлеуметтік желісінің әкімшілігінін атынан хабарландыру жіберіледі. Хабарландыруда: “ВК әлеуметтік желісіндегі парақшасы өз қызметін тоқтатты. Тоқтау себебі осы аккаунттан спам хабарландырулар таратылды. Парақшаны қайтадан бастапқы қалпына келтіру үшін астыдағы сілтеме бойынша өтіп, жаңадан логин және құпия сөз еңгізу керек”. Сенімділікті күшейту үшін қолтаңбаға ВК әлеуметтік желісінің белгішесі қойылады. ВК әлеуметтік желісінде досы екеуінің хабарландыруларын оқу мүмкіндігі ашылды. Оқу барысында тұратын мекен жайын, ортақ достарының есімдерін, бірге жиі баратын жерлерін, құрбысының есімін, ата анасы тұралы және т.б. ақпараттарды анықтау мүмкіндігі туды.

Келесі қадамда түнгі сағат 3:00-де хабарласу фактысы орындалады. Лақап есімі арқылы сәлемдесіп жиі баратын түнгі клубта барлық заттырын біреу ұрлап кеткені туралы оған хабарландырылады. Ортақ достарының есімдерін айтып хабарласқанда ұялы телефондарын алмағанын, құрбысы екеуі түнде қайта алмай тұрғанының анықталғаны жеткізілді. Бұл кездейсоқ адамның ұялы нөмірі екенін айтып, осы кісінің банктік картасына таксиге ақша салып жіберу туралы өтініш жасалды. Келесі күн қайтарып беремін,-деген уәде беріледі, әрине.

Зардап шегуші осындай алаяқтық іс- әрекеттерден кейін ақшаны банктік картаға 5 минут шамасында салып жіберді.

Претекстинг әдісінде адамның эмоциясына байланысты жасалғанына байланысты қарсы тұру қиын болып келеді. Дегенмен, Асхат өзінің мұқияттылығын танытқан кезде ВК парақшасынан келген хабарландыру жалған екенін көруі әбден мүмкін еді. Екіншіден, зиянкестің дауысы өзге болғандықтан досына қайта қоңырау шалу керек. Үшіншіден, тек екеулерін білетін сұрақ қойылуы тиіс.

Претекстингке қарсы тұру үшін, компания жұмыскерлері қоғамдық жүйелердегі өздерінің ақпараттарын азайтуы тиіс немесе ақпараттарына қол

жеткізе алатын адамдар санын шектеу тиіс. Қазіргі кезде көптеген қоғамдық жүйелерде өз ақпараттарыңды жасырын ұстауға мүмкіндік бар. Дегенмен, екінші әдіс (шектеу) осал болып келеді. Себебі, ақпаратқа қол жеткізе алатын адам арқылы құпия ақпарат ағып кетуі мүмкін.

2.3 Кво туралы кви

Кво туралы кви әдісі – бұл әдісте зиянкес, пайдаланушыға электронды пошта немесе корпортивтік телефон арқылы хабарласады. Зиянкес пайдаланушыға өзін техникалық көмек жұмыскері ретінде таныстырып, техникалық ақаулар болғанын хабарлайды. Келесі қадамда ол пайдаланушыға ақауларды жою керек екенін айтады. Одан кейін зиянкес, пайдаланушыны өз ыңғайына қарай қолданады. Мысалы, зиянды бағдарламаларды орнатуға немесе өзінің деректерін ашып беруге итермелейтін іс ірекеттер жасайды.

Кво туралы кви әдісіне жасаған зерттеу. Ең алдымен Кво туралы кви әдісіне зерттеу жүргізу үшін пайдаланушы таңдалады. Таңдаған жұмыскер IPSOS компаниясының бас бухгалтері. Енді қызметкердің жұмыс орны зерттеледі. IPSOS компаниясы консалтингтік компания болып табылады. IPSOS компаниясы қазіргі кезде халықаралық компания болып табылады. IPSOS компаниясының басты мақсаты әріптестеріне зерттеу жұмыстарын өткізу. Ол анкета немесе сұрау түрінде болады. IPSOS компаниясының қазіргі әріптестері зерттеледі. Зерттеулер жүргізген кезде, IPSOS компаниясы Coca Cola, KFC, Monster компанияларынан тапсырыстар алған [9].

Келесі қадамда IPSOS компаниясының жұмыскеріне алдын ала дайындалған хабарландыру жіберіледі Хабарландыруда өзіңді техникалық қызмет көрсету маманы ретінде таныстырасың. Біздің тарапымыздан KFC компаниясының электронды поштасына ұқсас пошта құрылып, IPSOS компаниясынын бас бухгалтеріне хабарландыру жіберіледі. Хабарландыру ішінде болашақта өткізетін сұрауларда өзгертулер бар деп жазылған. Өзгертулерді сілтеме арқылы көруге болатынын ескерту қажет.

Сілтемеде өзіміз құрған өзгертулер және зиянды бағдарлама болды. Сілтеменің батырмасын басқан кезде винлок вирусы қосылып, экранды блоктайды. Винлок вирусы винлобуайлдер бағдарламасы арқылы құрылған. Енді IPSOS компаниясының бас бухгалтері ақаулықты шешу мақсатында бізді шақырады. Біз вирусты өшіру үшін алдымен пайдаланушы идентифифкаторларын білу қажет екенін айтамыз. Келесі қадамда IPSOS компаниясының жұмыскері бізге өзінің корпоративтік идентификаторларын айтты. Алынған идентификаторлармен мен кез келген товарды компания атынан сатып ала алатын мүмкіндікке ие болдық.

Енді Кво туралы кви –ді талдаймыз:

- қызметкерге өзіңді таныстырасың. Есінде қалатындай біздің тарапымыздан әрекеттер жасалады.

- қызметкер бізді шақыру үшін әрекеттер жасалады. Вирус арқылы компьютеріне шабуыл жасалады.

- қызметкер өз қолымен бізге идентификаторларын беру үшін әрекет жасалады.

- Кво туралы кви жүзеге асты. Жұмыскердің вирусы жойылды (вирусты өзіміздің енгізгеніміз белгілі). Жұмыскер бізге өзінің идентификаторын берді.

Бас бухгалтер алдану себебі, адамға деген сенімділігі. Біз IPSOS компаниясының жұмыскері болғандықтан бізден олар ондай алаяқтық күткен жоқ. Бұндай ақаулықтар адамның мінез құлқына тән. Бас бухгалтердің жасаған қателігі - идентификаторларын айтпауы тиіс еді.

Осындай ақаулықтардың алдын алу үшін қауіпсіздік саясаты қажет. Қазіргі кездегі компаниялардың 80%-да қауіпсіздік саясаты жоқ. Қауіпсіздік саясаты өте қажет зат болып табылады. Қауіпсіздік саясатында жұмыскер өзін қалай ұстау керек екені жазылады. Бас бухгалтерге келсек ең басында қауіпсіздік саясатымен жұмысын орындаған кезде алдымен хабарландыру жіберушіні айқындап алу керек еді. Екіншіден, бұндай тақырыптағы хабарландырулар бас бухгалтерге келмеуі тиіс. Хабарландыру келген жағдайда белгілі жұмыскерге айтуы қажет еді. Дегенмен хабарландыруды ашқан жағдайда идентификаторларды ешкімге айтпау қажет. Техникалық қызмет көрсету жұмыскері болса да, жұмыскерге айтпай бас бухгалтер жеке енгізуі керек.

Кво туралы кви әдісіне компания қарсы тұру үшін, жұмыскерлерді жаңа жұмыскермен таныстыру қажет. Компанияда ақ тізім жасалуы керек, сонда тек авторизациядан өткен телефондар ғана қоңырау шалу мүмкіндігіне ие болады.

2.4 Трояндық вирус және жолдағы алма

Трояндық вирус – бұл әдіс пайдаланушының эмоцияларына негізделген. Мысалы, қорқыныш, қызығушылық таныту және тағы да басқа. Зиянкестің хатында антивирустың жаңартылуы, ақшалай ұтысқа кілт немесе жұмыскерге сыйлық болуы мүмкін. Шын мәнінде хабарламада зиян бағдарлама орналасқан. Пайдаланушы бағдарламаны қосқан кезде, бағдарлама компьютерден керек ақпараттарды ұрлайды.

Жолдағы алма әдісі трояндық вирусқа ұқсас келеді. Бірақ вирус физикалық тасымалдаушыларда болады (CD, флэш жинағыш және тағы да басқа). Зиянкес әдетте тасымалдауышты қол жетімді жерлерде сақтайды (көлік тұрақтары, асхана, жұмыс орындары, дәретхана және т.б.). Пайдаланушы тасымалдаушыға көңіл аудару үшін, тасымалдаушыға компания логотипін немесе басқа жазуларды жазу мүмкін. Мысалы, “сатылым тұралы деректер”, “жұмыскерлердің жалақысы”, “салық тұралы ақпарат” т.б.

Мысалы, зиянкес компания белгісі жабыстырылған диск тасымалдаушыны қол жетімді жерге тастап кетеді. Диск тасымалдаушыға 2012 жылғы жұмыскерлер жал ақысы тұралы ақпарат деп жазба жабыстырады. Жұмыскер

дискті алып өз компьютеріне салуы мүмкін, себебі адамның қызушылығы ол мінез құлық осалдылығы. Зардап шегуші вирусы бар диск тасымалдаушыны компьютерге салған кезде вирус компьютерге енеді және зиянкес компьютерге қашықтықтан қол жеткізе алады. Зиянкес компьютерге немесе компьютерлік жүйеге зардап алып келе алады.

2016 жылы өткен зерттеулерге сай Иллинойс университетінің кампусынын жан жағына 297 флэш тасымалдаушы қойылған. Дискте вирус бағдарламалары болған. Зертеудің нәтижесінде 297 флэш тасымалдаушының 290-ы демек 98%-ы алынған. Ал 135 флэш тасымалдаушы вирусты жүзеге асырған [10].

Трояндық вирус әдісіне және жолдағы алма әдістеріне мысал- трояндық вирус әдісі, аты айтып тұрғандай трояндық вирустар арқылы жүзеге асырылады. Трояндық вирустардың көптеген түрлері бар. Мысалы, қашықтықтаң рұқсатсыз қатынас жасайтын, деректерді жоятын, деректерді жазатын, қауіпсіздікті сақтайтын бағдарламмаларды өшіретін және т.б. Дипломдық жұмыста трояндық ат әдісінде қашықтықтан рұқсатсыз қатынас жасайтын вирус қолданылады.

Ең алдымен зерттеу жұмысы болатын аумақ таңдалады. Таңдалған аумақ - жастар кітапханасы. Жастар кітапханасының компьютерлік бөлімшесінде вирусы бар флэш тасымалдаушыны жұмыс столының үстіне қойып кеттік делік.

Флэш тасымалдаушының ішінде қашықтықтаң рұқсатсыз қатынас жасайтын вирусты енгіземіз. Зардап шегуші ол вирус екенін анықтап қоймауы үшін оны суретке жабыстырып салдық.

Ол үшін ең алдымен вирусты, суретті және байланысты файлдарды архивтау қажет. Енді блокнот бағдарламасын ашып «copy /b 1.jpg + 1.rar 2.jpg» деген кішігірім код жазылдм. Бұл код вирус және вирусты тығатын сурет екеуін қосып 2.jpg атты сурет құрады. Суретті bat форматында сақтап іске қосу қажет. Қосқан кезде суреттің өзі ашылады. Бірақ қалған файлдар іске қосылады. Қосылған файлдарды диспетчер задач арқылы көрсе болады. Суретте қандай вирус бар екенін білу үшін оны архиватор арқылы ашу керек. Бағдарлама дайын.

Келесі қадамда, зардап шегуші флэш тасымалдаушыны алып кетуін немесе кітапханада іске қосуын күту қажеттілігі туындайды. Зардап шегуші флэш тасымалдаушыны кітапханада өзінің ноутбугіне салды. Флэш тасымалдаушыда тек қана бір опера браузері болғандықтан оны іске қосқан жоқ. Қасындағы досы флэш тасымалдаушыны сұрап алды. Флэш тасымалдаушының ішіндегі вирусты іске қосты. Біз зардап шегушінің ноутбугімен толығымен басқара аламыз. Вирус қосылған және вирус жазылып алынды деген ақпаратты алмады. Вирус білінбей С дискте жаңа папка ретінде сақталады. Вирус арқылы зардап шегушінің ноутбугімен басқару мүмкіндігіне ие бола аламыз. Бірақ ол үшін зардап шегуші ноутбугімен пайдаланбауы тиіс. Егер пайдаланушы активті болса, оның іс қимылдары бірінші кезекте орындалады. Сол үшін пайдаланушы ноутбукпен жұмыс істемей отырған кезде, электронды құралымен не істегің келеді соны істеуге болады.

Біз зардап шегушінің компьютеріне кіріп, вирустың тұрған жерін қарай аламыз.

Тасымалды алма әдісінен қорғану амалдары:

- бөтен адамның флэш тасымалдаушысын алмау тиіс;
- біреудін флэш тасымалдаушысын алған жағдайда, флэш тасымалдаушыны тазалау арқылы бастапқы қалпына келтіру керек;
- тазартудан өтпей ашатын жағдайда, флэш тасымалдаушының ішіндегі бағдарламалар немесе фото, видео және т.б. виртуалды машина ішінде ашылуы тиіс. Вирус болған жағдайда виртуалды машинаны өшіріп, сонғы сақтау болған уақытқа қосамыз. Бұл шаралады жүргізбеген жағдайдада, зиянкес тек виртуалды машинаны бұза алады. Компьютерге ешқандай қауіп төнбейді;
- басқа компьютерлерде қосып тексеру. Яғни өзінің емес, мысалы комьютерлік клуб немесе кітапханадағы компьютерлерде тексеріп алу қажет.

Кері әлеуметтік инженерия – бұл әдіс пайдаланушы, зиянкеске өзі көмек сұрауға итермелейтін әдіс болып табылады. Кері әлеуметтік инженерия тұралы, пайдаланушы зиянкеске ақпаратты өзі берген кезде айтады. Бұл ойға қонымсыз болып көрінсе де, бірақ шын мәнісіне келгенде, техникалық немесе қоғамдық салада беделі бар адамдар, жиі пайдаланушылардың идентификаторлары және көптеген құпия ақпараттарын алады, себебі ешкім беделді адамдардаң күмәнданбайды. Мысалы, қолдау көрсету қызметкерлері, сізден ешқашан индентификаторларынызды немесе құпия сөзді сұрамайды. Бірақ көптеген пайдаланушылар өздерінің құпия ақпараттарын, мәселенің тез шешілу мақсатында береді. Демек, зиянкес пайдаланушыдан құпия ақпараттарын сұраған жоқ.

Кері қоғамдық инженерияға мысал: идентификаторларды қалай оңай алып алуға болатынын көрсетеді. Сізге желілік администратор жексенбі күні сағат таңғы 8:00 қоңырау шалады. Желілік администратор қазір бізде техникалық жұмыстар болып жатыр, қиын түсініксіз терминдер айтады, қазір келе аласыз ба сіздің компьютеріңізді ашу керек болып жатыр деп айтады. Сіз ішіңізден «Жексенбі күні таң атпай бір минуттық жұмыс үшін барып жүремін бе? Тез арада, мәселені шешетін басқа жолдар бар ма?» -деп сұрайсыз. Әрине бар, сіз маған идентификаторларынызды беріңіз (логин, құпия сөз) мен кіріп бүкіл мәселелерді шешемін, дүйсенбі күні келіп идентификаторларыңызды өзгерте аласыз деп айтады. Сіз ашық жүрекпен қуана қуана логин, құпия сөзіңізді системдік администраторға бересіз де ары қарай ұйықтайсыз. Сенгісіз, бірақ бұндай алаяқтыққа 70 пайыз адам түседі. Демек зиянкес 10 адамның нөмірлерін тауып, қоңырау шалса 6-7 адам өзінің логин, құпия сөздерін береді. Себептері оңай, хакер алдмен бәрін нашар тұрғыдан көрсетеді (жексенбі, таңғы сағат 8:00, тездетуліктің итермелеуі). Сіз ойланып баруға тура келеді деген шешімге келдіңіз, ал енді күтпеген жерден сізге келмейтін және мәселені оңай шешуге болатын нұсқа айтады. Әрине көп адамдар келіседі.

2.5 Ақпараттарды ашық көздерден іздеу

Ақпараттарды ашық көздерден іздеу әдісі – қоғамдық инженерияны қолдану үшін, тек психология саласындағы қабілет жеткіліксіз, қолдану үшін адам тұралы ақпаратты іздеу қабілетті де өте маңызды. Ақпаратты алудың жаңа түрлерінің бірі болып осы әдіс саналады. Ақпаратты көбінесе қоғамдық жүйелерден алады. Мысалы, livejournal, «Одноклассники», «ВКонтакте» секілді парақшаларда үлкен ауқымдағы ақпараттарын адамдар жасырмайды. Әдетте, адамадар қауіпсіздікке аса көңіл бөлмейді. Ақпараттарын қол жетімді жерде қалдырып, зиянкес онымен қолдана алады деп ойламайды. Мысалға, Евгений Касперскидің баласының ұрлануын айтса болады. Зерттеулер көрсеткендей, зиянкестер баласының сабақ кестесін және үйге жүретін жолдарын қоғамдық жүйелерден біліп алған.

Қоғамдық жүйедегі ақпараттарын сырт көзден құпия ұстаған адамдар, ақпараттары зиянкестің қолына түспейтініне сенімді бола алмайды. Мысалы, бразильдік инженердің зерттеулері көрсеткендей, кез келген адамның досы болу үшін, тек 24 сағат жеткілікті. Зерттеулер кезінде Нельсон Новаес Нето жәбірленушіні таңдап, жәбірленушінің қасындағы адамның парақшасын құрды. Алдымен зиянкес, жәбірленушінің достарына дос болуды ұсынған. Парақшаны құрған уақыттан бастап жәбірленуші зиянкестің достығын қабылдауына дейінгі уақыт 7,5 сағат болған. Осылайша зиянкес, пайдаланушы сырт көзден сақтаған ақпараттарына қол жеткізді [11].

Ақпараттарды ашық көздерден іздеу әдісіне жасалған мысал. Бірнеше ақпарат жинайтын адам таңдалады, айталық таңдалған адам - Сейлова Нургуль Абадулаевна.

Аты- жөні белгілі. Сейлова Нургуль Абадулаевна.

1979 жылы Қызылорда облысында дүниеге келген.

2001 жылы КазНИТУ жоғарғы оқу орнын бітірген.

2014 жылдан бастап КазНИТУ-нің ИИиТТ институтының ақпараттық қауіпсіздік кафедрасының жетекшісі.

Келесі қадамда e-lib сайтында Нургуль Абадулаевна 53 публикация жасағанын көруге болады. Публикациялар 2011 жылдан – 2017 жылдар арасында жүргізілген. Осы уақыт арасында жұмыс орны КазНИТУ деп белгіленген. Демек осы аралықта КазНИТУ-да жұмыс істеген деп ойлауға болады.

Келесі қадамда, Қазақстанның ішкі істер министірлігінің сайтына кіріп тұратын мекен жайын білу мүмкіндігі пайда болды.

«Мкр.Мамыр 4, дом 295, кв 41».

Көршісі Касымова Жубаныш Ишангалиева, Коптилеуова Дина Тургалиевна, Икранбеков Алмас Зубайрович.

«Устройство защиты от несанкционированного доступа» атты жобаға қатысты, АО Фонд Науки-ден қаржыландырылған грантты иемденген.

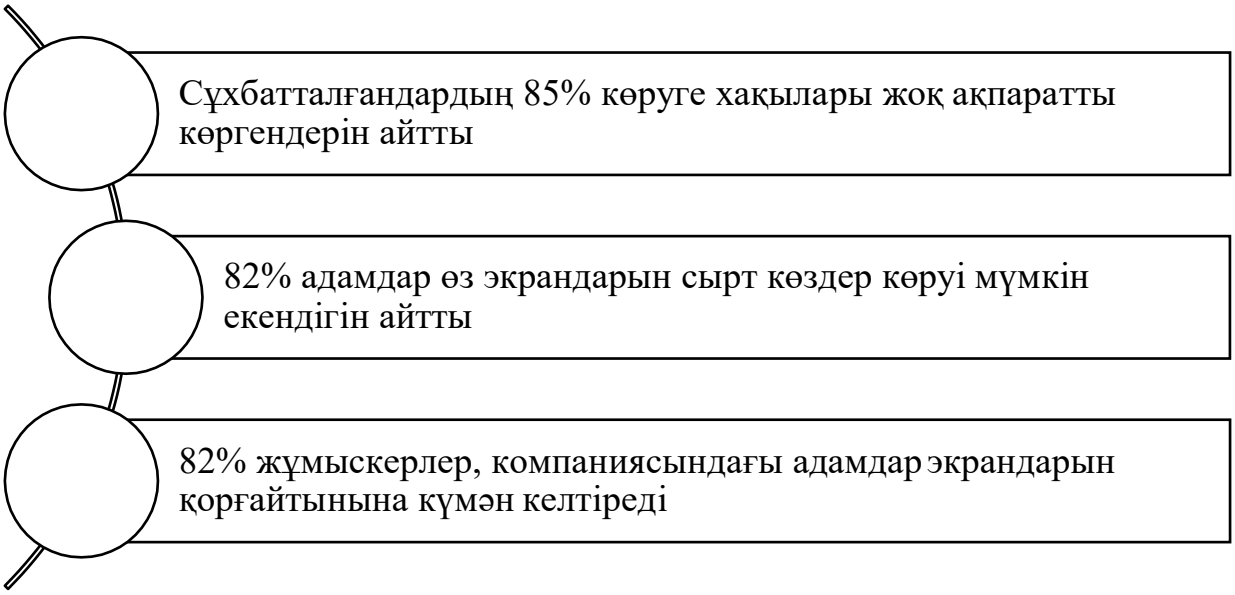
Үйінің телефон нөмірі 87272396390. Ұялы телефоны 87073505038. Поштасы seilova_na@mail.ru. Каспи банкінің, каспиголд картасымен қолданады. Картаның соңғы сандары 5687.

Әсер ету механизмдер әдісі – бұл әдіс социалді инженерлердің ең сүйікті және ақпаратты толық беретін түрлерінің бірі болып табылады. Бұл әдістің негізгі амалы, адамдардың психологиялық әлсіздігін қолдану арқылы керек ақпаратты алу. Мысалы, өзара ауысу амалы. Бұл амалдың өте көп түрлері бар. Біреуіне мысал келтірейін, сіз ұзын кезекте тұрсыз. Ен алдында ерте келген кісі тұр. Кісінің көңіл күйі түсіріңкі екенін байқадыңыз. Кезектің алдында тұрған кісіге келіп, шоколад ұсынасыз. Көңіл күйіңізді көтеру үшін деп айтасыз. Біраз уақыттан кейін, өтірік жүйкеніз тозып сағатқа жиі қарайсыз. Бір жерге кешігіп бара жатқандай кейіп танытасыз. Келесі қадамда, сіз шоколад берген кісі сізді байқап сізге өз кезегін береді. Бұл әдіс қауіпсіз әдістердің бірі болып табылады.

Әсер ету механизмдерінің тамашалығы, ол жеке адамға және топтарға да қолдана алуында.

Адамның эмоционалды күйімен басқару әдісі – қоғамдық инженерлерлердің қолданатың басты әдістерінің бірі болып табылады. Кездесулер жүргізген кезде немесе жай диалог жүргізген кезде, адамға әр түрлі эмоция бере алатын адам әңгімені басқарады. Зиянкестер бұл заңдылықты өте жақсы біледі және өкінішке орай кенінен қолданады. Ең көп кездесетіні, адамға аяушылық, жанашырлық немесе күнәлік сезімдерді сездіру. Көбінесе бұл амалдар іске асуы ең жоғары болып табылады. Мысалы, жолда бір кісі балама тамақ алып беру үшін ақшалай көмектесіп жібересіз бе? деп сұрағанда бермесен бір түрлі сезім туындайды. Егер бөтен адам келіп, сізді әр түрлі эмоцияға баулайтын іс әрекеттер жасаса, бұл адамнан сескену керек. Бұндай әдіс өте оңай ашылады, ол үшін EQ-ді өсіру керек.

Йықтық серфинг әдісі – бұл әдіс аты айтып тұрғандай, адамның құпия ақпаратын артынан тұрып бақылау. Бұл әдіс көбінесе қоғамдық жерлерде кездеседі (кафе, парк, әуе-жай, сауда орталығы). Сондықтан құпия ақпараттарды немесе корпаративтік ақпараттарды қоғамдық жерлерде оқуға болмайды.

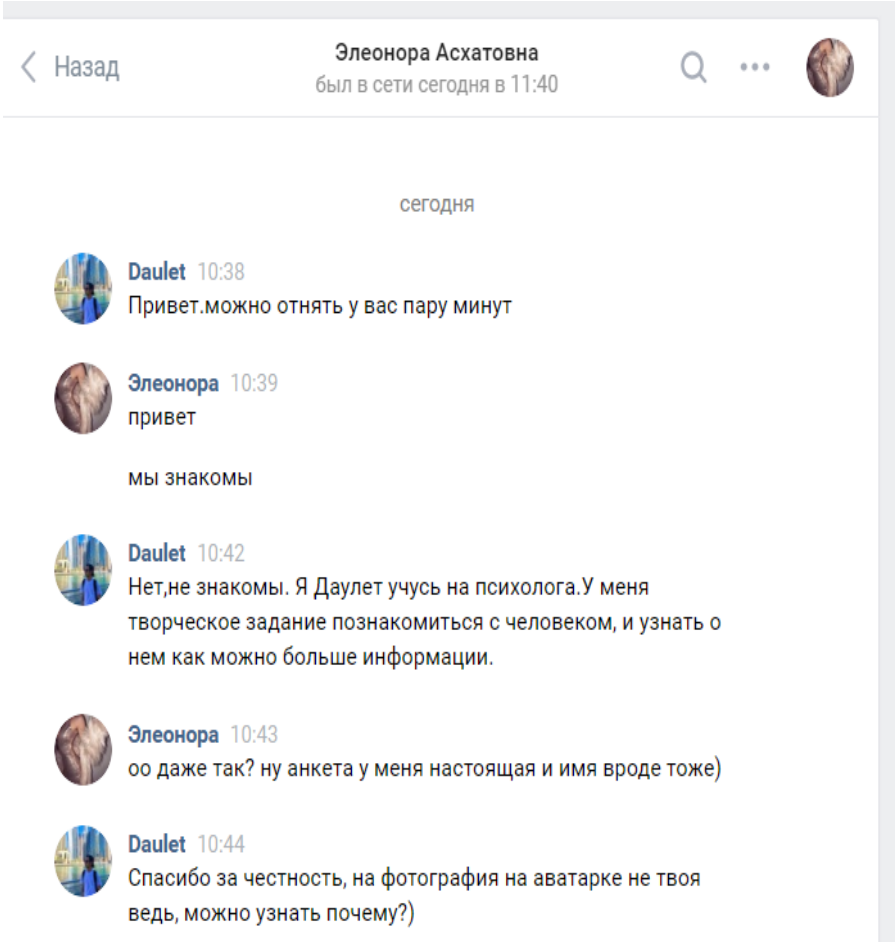


2.1 сурет – IT мамандарының қауіпсіздік тұралы зерттеулерінің нәтижесі

3 Әлеуметтік инженерияға іс жүзінде эксперимент жасау

3.1 Әлеуметтік инженерияның бірінші тәсілі - адам сеніміне кіру

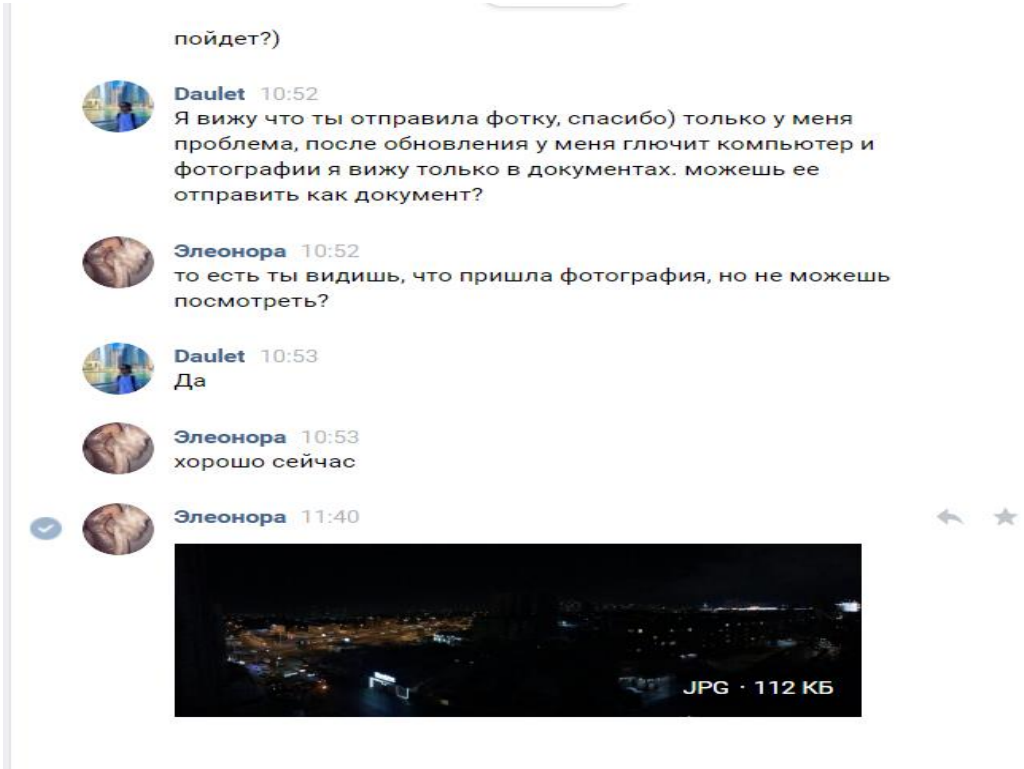
Бұл тәсілді қолдану барысында «Вконтакте» әлеуметтік желісінде шабыл жасалынатын нысан (Элеонора Асхатовна) таңдалынды. Сенімге кіру үшін хат алмастық.



3.1 сурет – Хат алмасу процессі

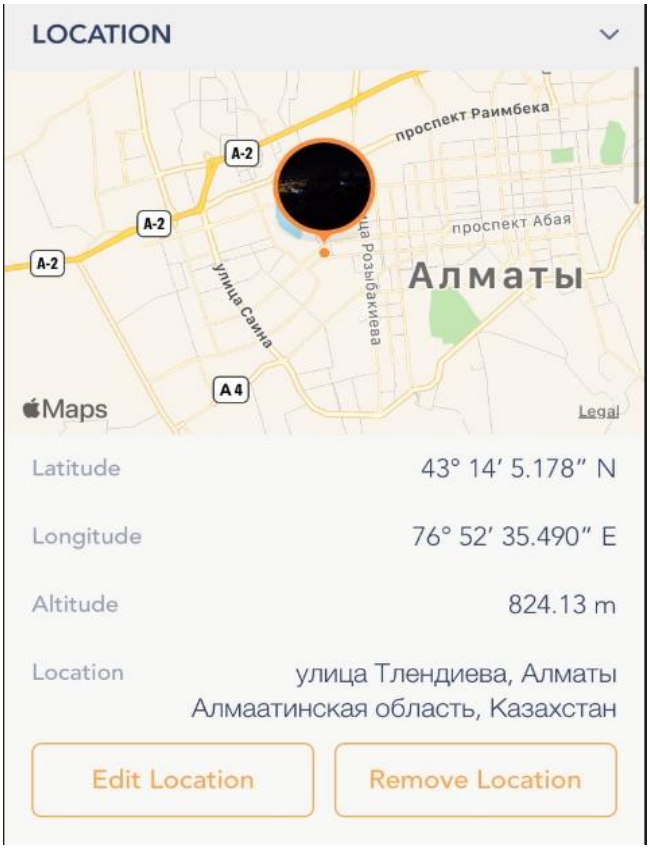
Кейін нысанның сеніміне кірген кезде, бізге керекті құжаттар сұралды. Сол құжат арқылы бізге керекті ақпараттарға қол жеткізетін боламыз (3.1-3.2 сурет).

3.2 сурет – Қол жеткізілген құжат

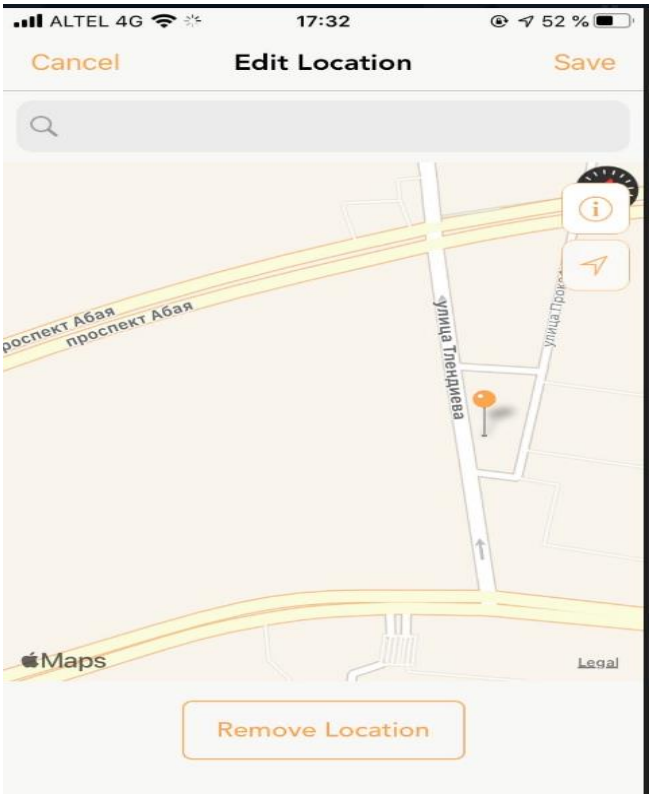


3.3 сурет – Қол жеткізілген құжат (JPG форматта)

Келесіде біз құжатты пайдалана отырып, нысанның суретті түсірген мекенжайы туралы ақпарат аламыз.

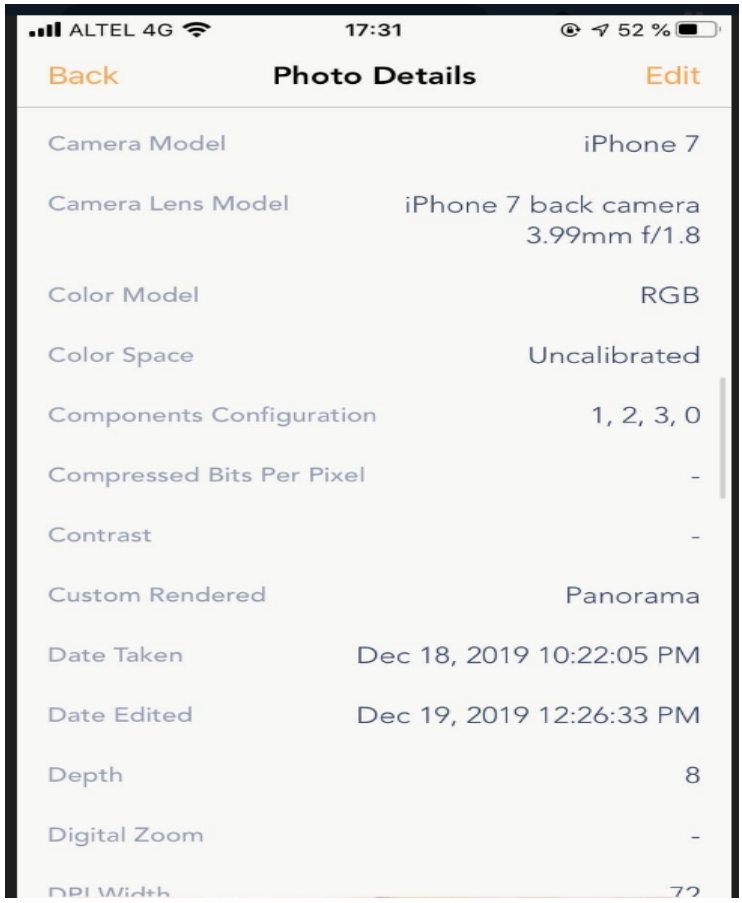


3.4 сурет – Нысанның мекежайы



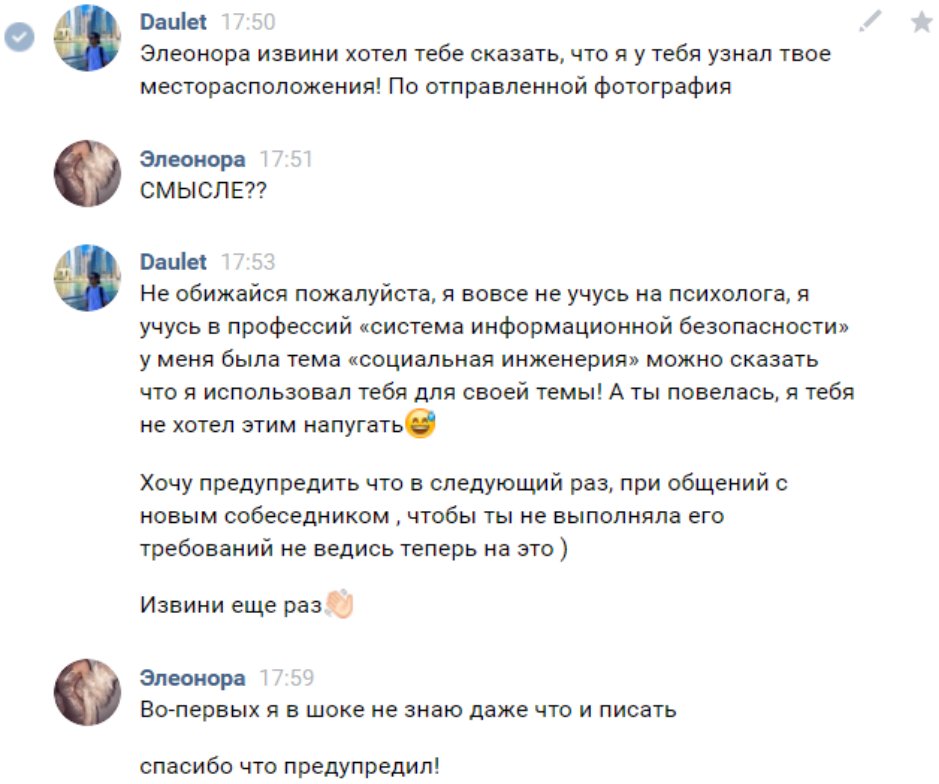
3.5 сурет – Нысанның мекежайы

Сонымен қатар қолданылатын ұялы телефоны жайында ақпарат алдық.



3.6 сурет – Қолданылған ұялы телефон жайында ақпарат

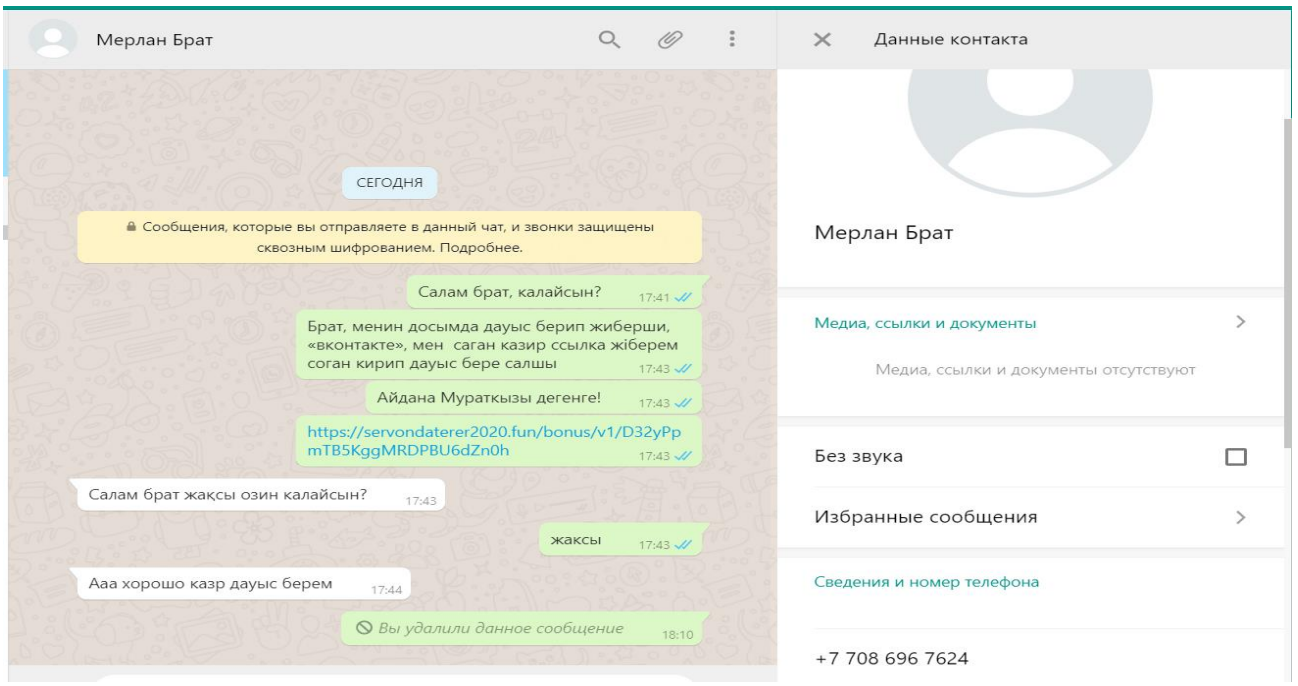
Бұндай шабуылдан қорғану әрекеті ретінде бейтаныс адамдарға мәліметтерді айта бермей ұсынылады. Себебі шабуылдаушы сіздің берген мәліметтеріңізді қарсы әрекеттер үшін қолдану мүмкін.



3.7 сурет – Қорғану шаралары

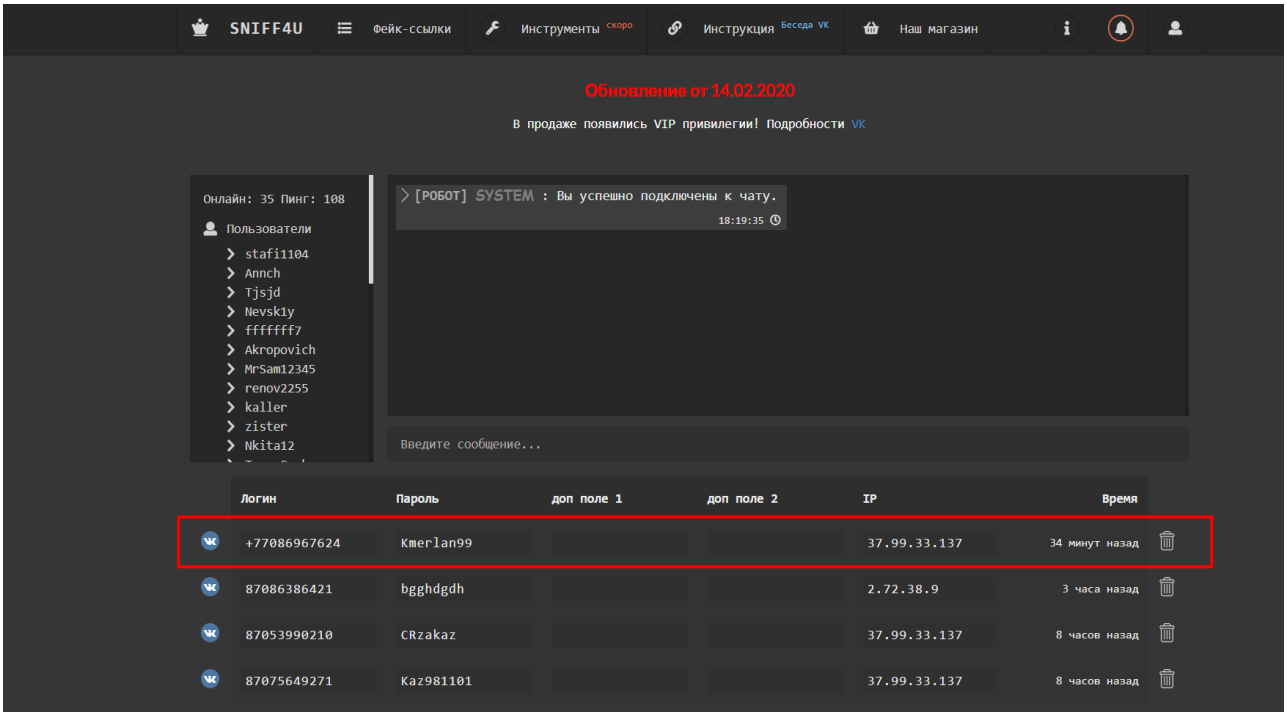
3.2 Әлеуметтік инженерияның екінші тәсілі - фишинг сайт

Сенімге кіру мақсатында хат алмасу процесі жүргізілді. Бұл тәсілде нысанға арнайы сілтеме жіберілді.



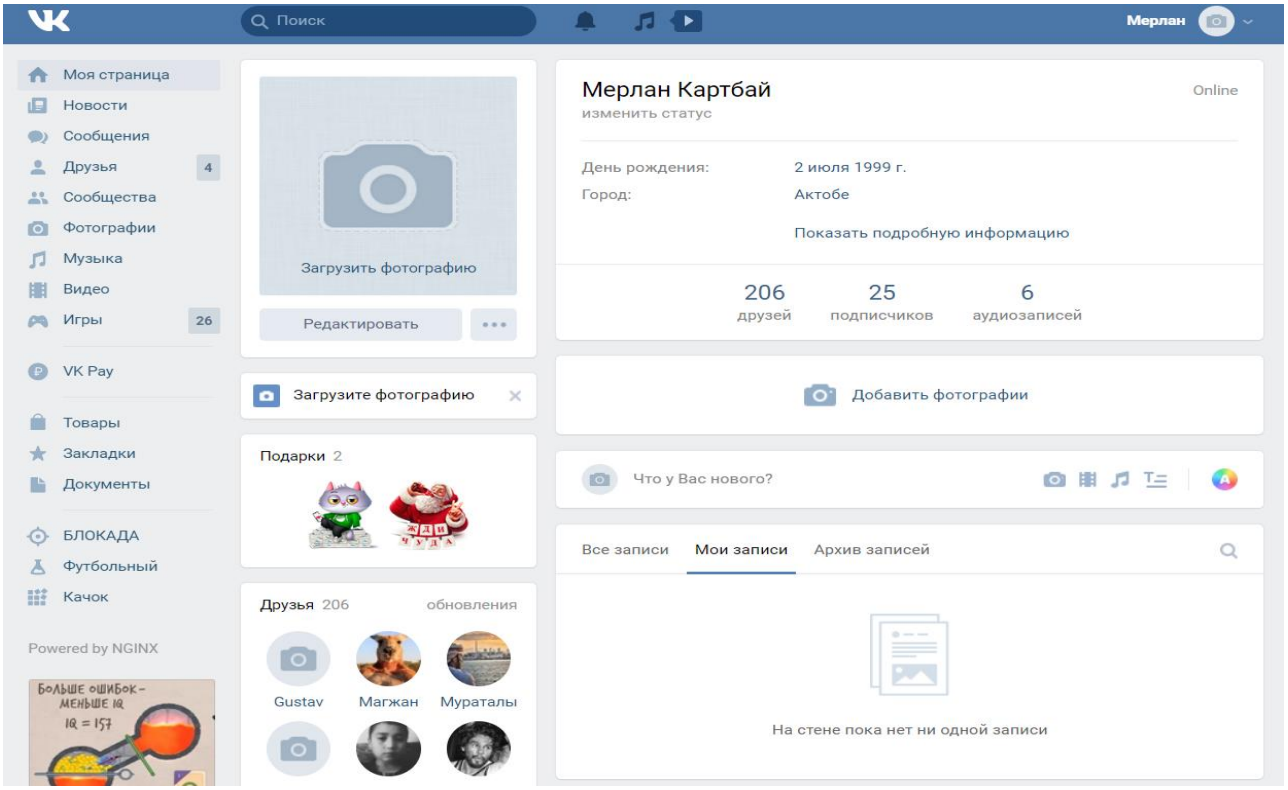
3.8 сурет – Сілтемені ұсыну

Кейін нысан бізге керекті сілтеме арқылы біз дайындап қойған сайтқа кіріп тіркеледі. Соның нәтижесінде біз нысанның жеке мәліметтеріне (логин және құпия сөз) қол жеткіздік.



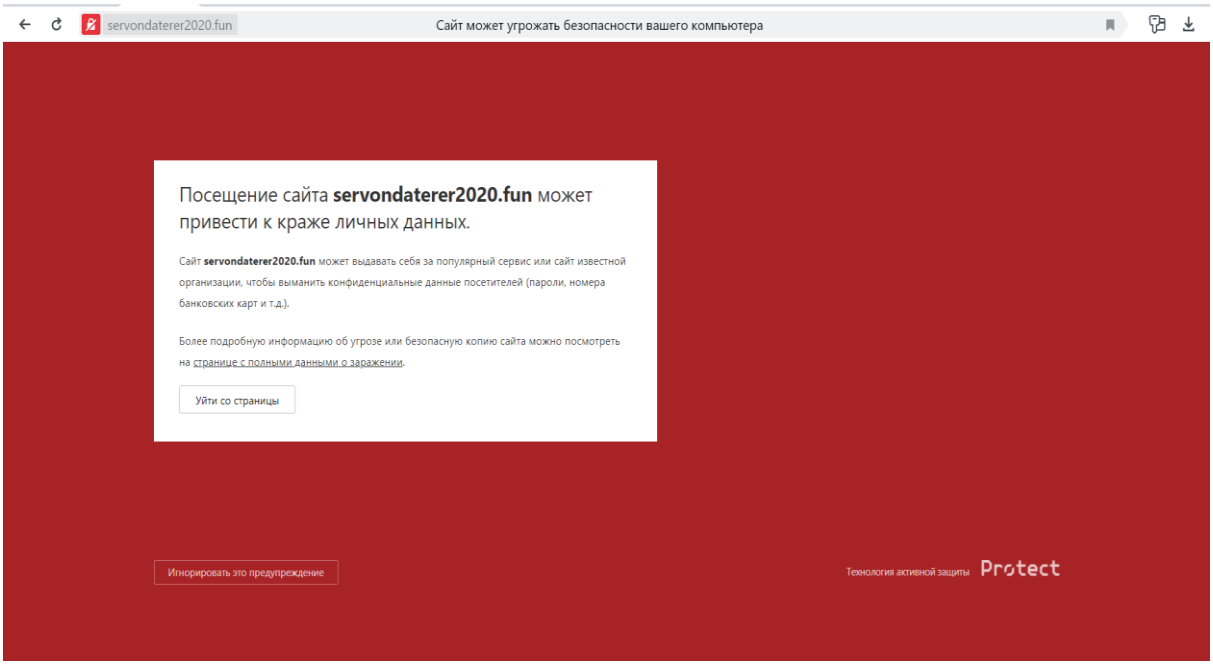
3.9 сурет – Қол жеткізілген құпия деректер

Біз нысанның жеке мәлемттерін пайдаланып «Вконтакте» әлеуметтік желісінде сәтті авторизация процесін өтіп, нысанның парақшасынан кірдік.



3.10 сурет – Сәтті авторизация процессі

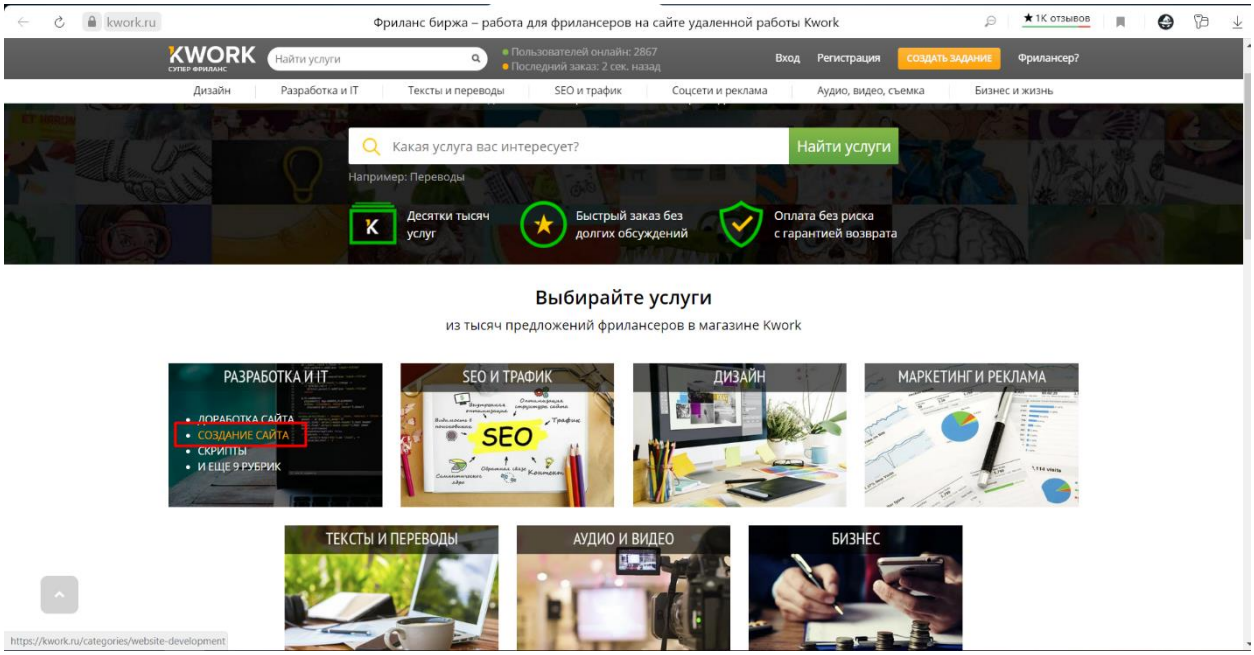
Бұндай сайттық фишинг шабуылынан қорғану амалы ретінде, антивирус бағдарламасын орнатуды ұсынамыз. Ол сенімсіз сайттарға кірер алдында ескертеді және алдын алады.



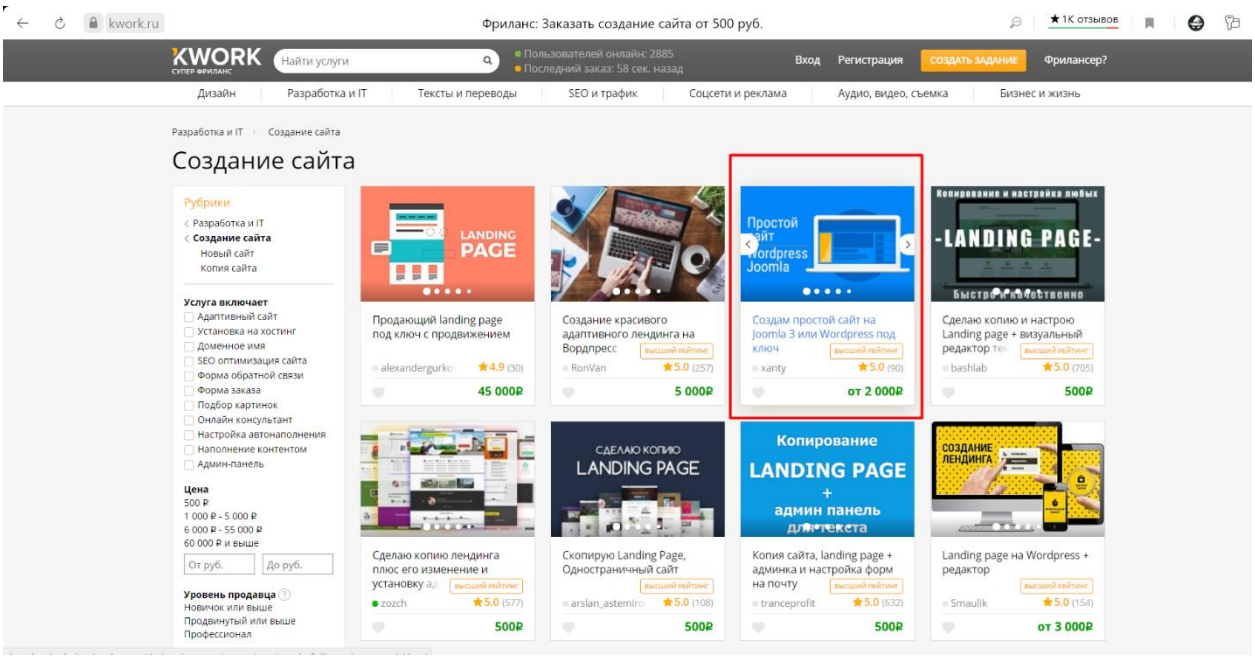
3.11 сурет – Антивирустың қорғау шаралары

3.3 Әлеуметтік инженерияның үшінші тәсілі – «Кво туралы кви» әдісі

Ең алдымен нысанды «Kwork.ru» сайтынан іздейміз, ол үшін өзіміз жасайтын жобаларды және қызметке тапсырыс жарнамасын таңдаймыз.

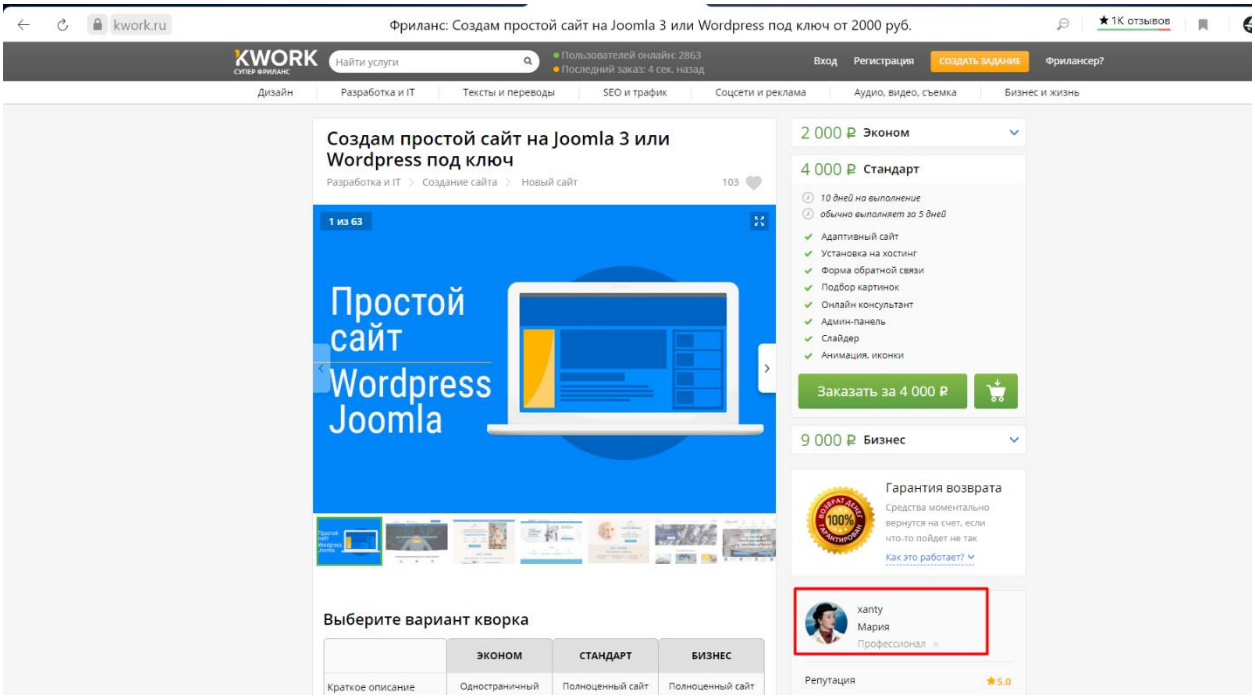


3.12 сурет – «Kwork.ru» сайты



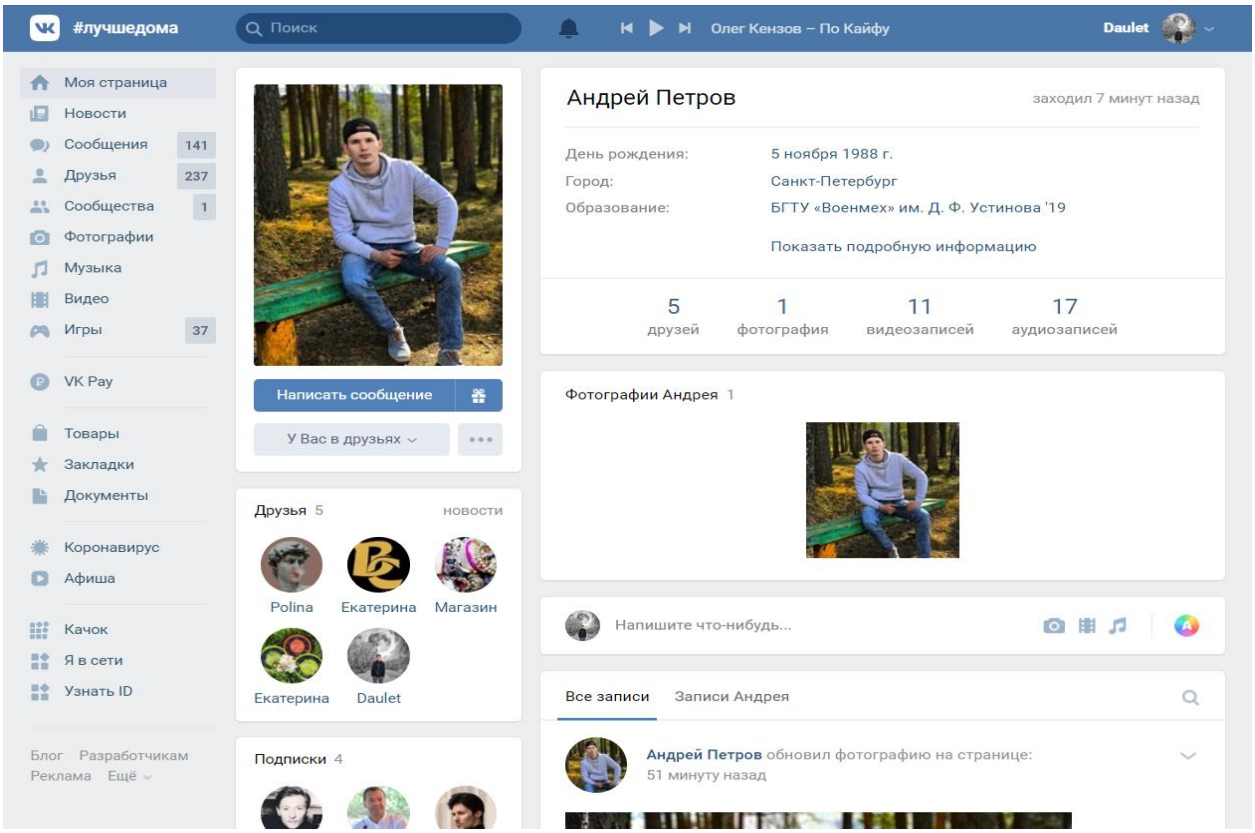
3.13 сурет – Қызметкеттер жарнамасы

Қызмет керекті нысанды анықтап, оның әдеуметтік желідегі парақшасына өтеміз.

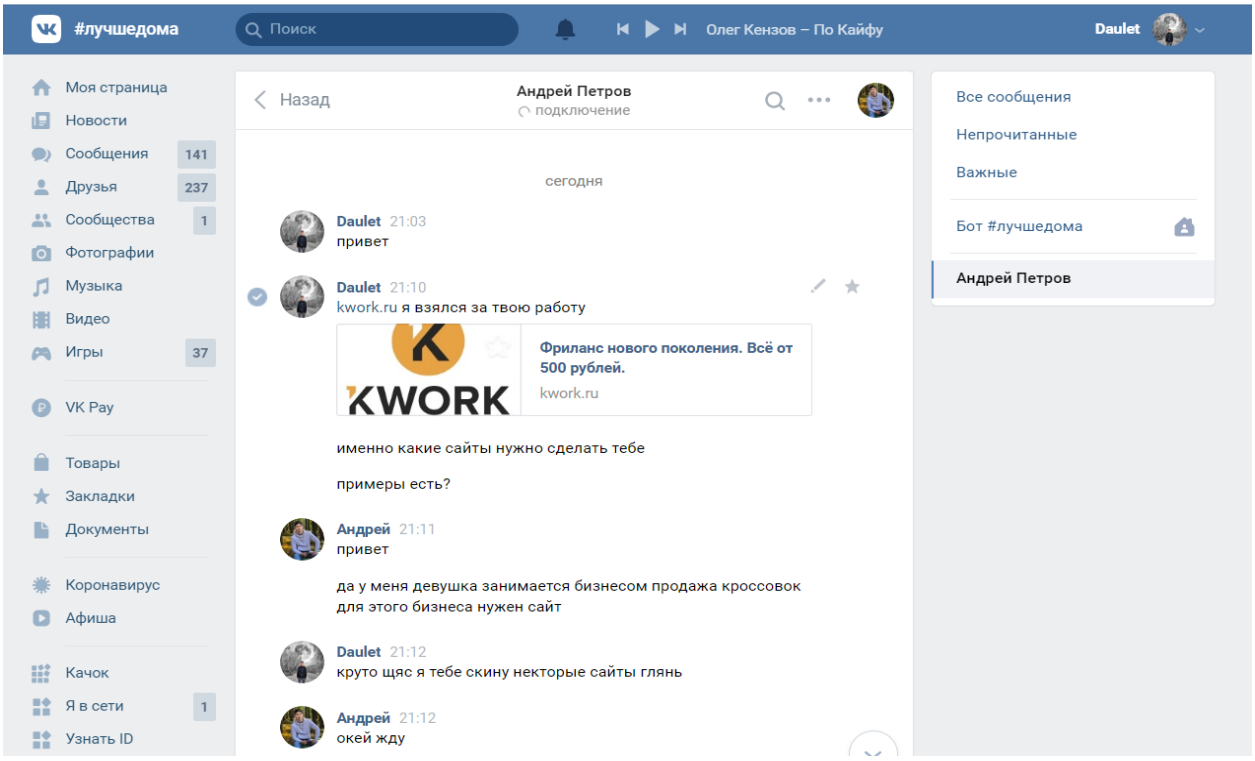


3.14 сурет – Нысанды анықтау

Нысан туралы барлық керекті ақпараттарды іздестіріп, сеніміне кіріп, хат алмасамыз.

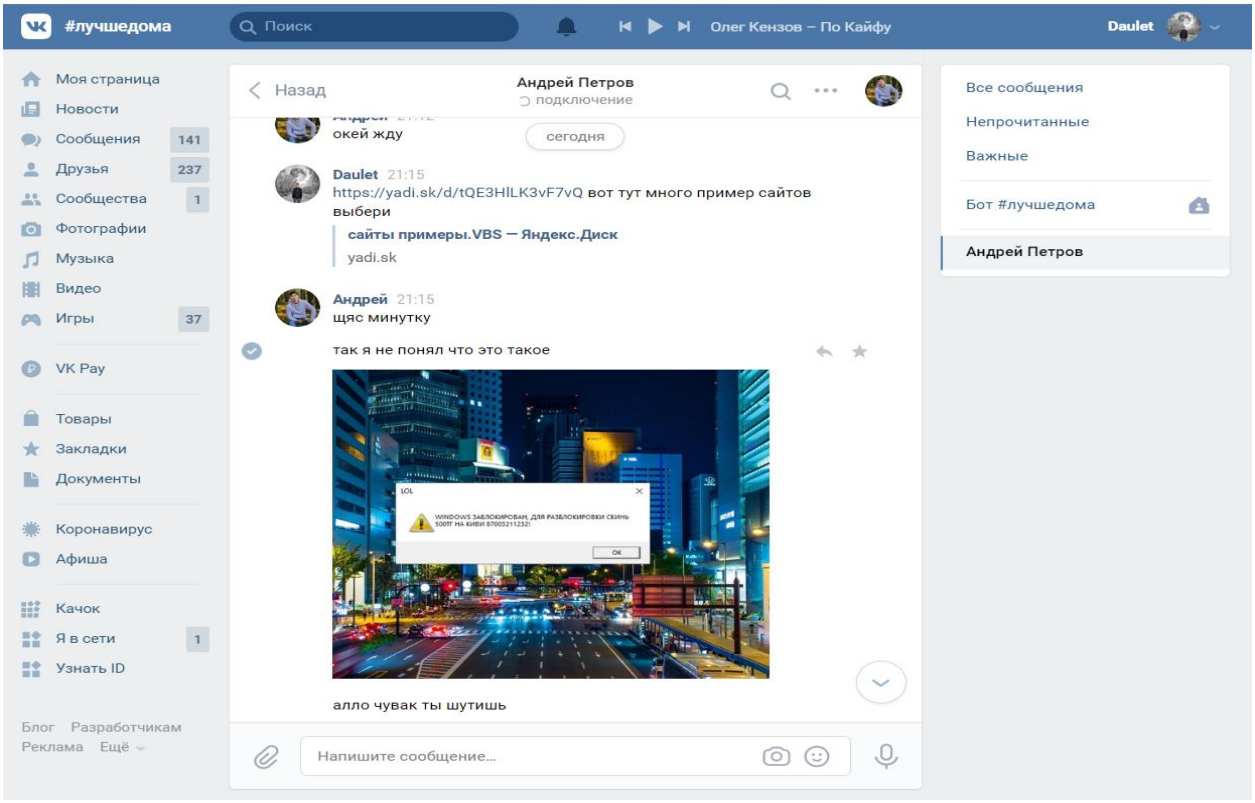


3.15 сурет – Ақпарат жинау



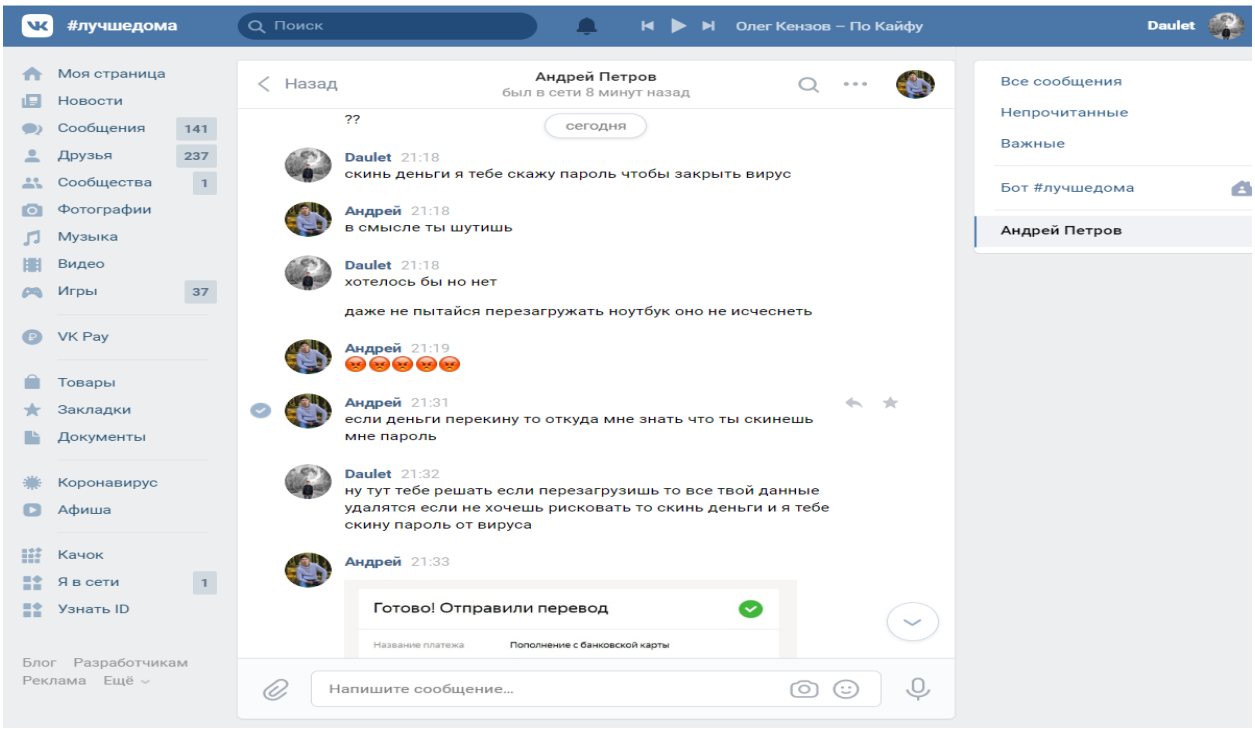
3.16 сурет – Өз қызметімізді ұсыну

Келесіде өнімдерімздің түрлерін көрсету мақсатында нысанға вирусталған jbs форматындағы деректеріміздің сілтемесін жібереміз. Қызығушылығы оянған нысан басқа да жұмыстарды салыстырып көру мақсатында деректерді жүктейді. Деректер компьютер жадына жазылған сәтте вирус қосылады. Нәтижесінде компьютердің экран бетінде хабарлама пайда болады.

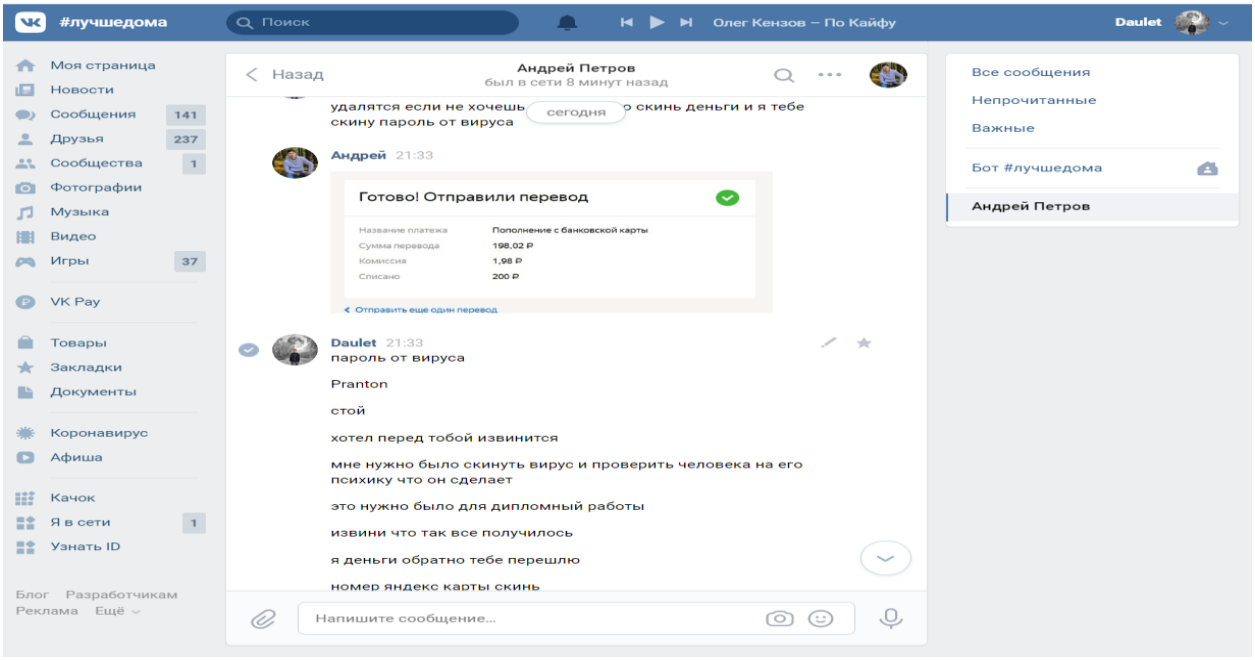


3.17 сурет – Вирус туралы хабарлама

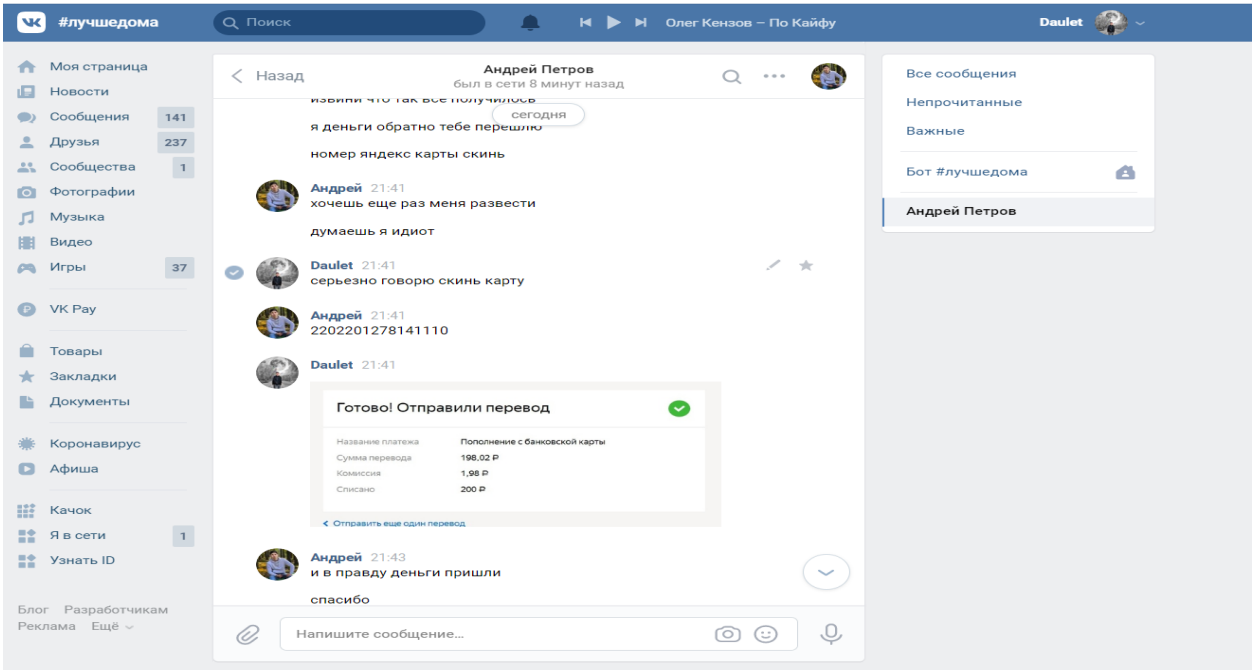
Бұл хабарламада Windows жүйесінің бұғатталғаны жөнінде, егерде керекті соммадағы төлемді жасамайынша бұғаттың ашылмайтыны айтылады.



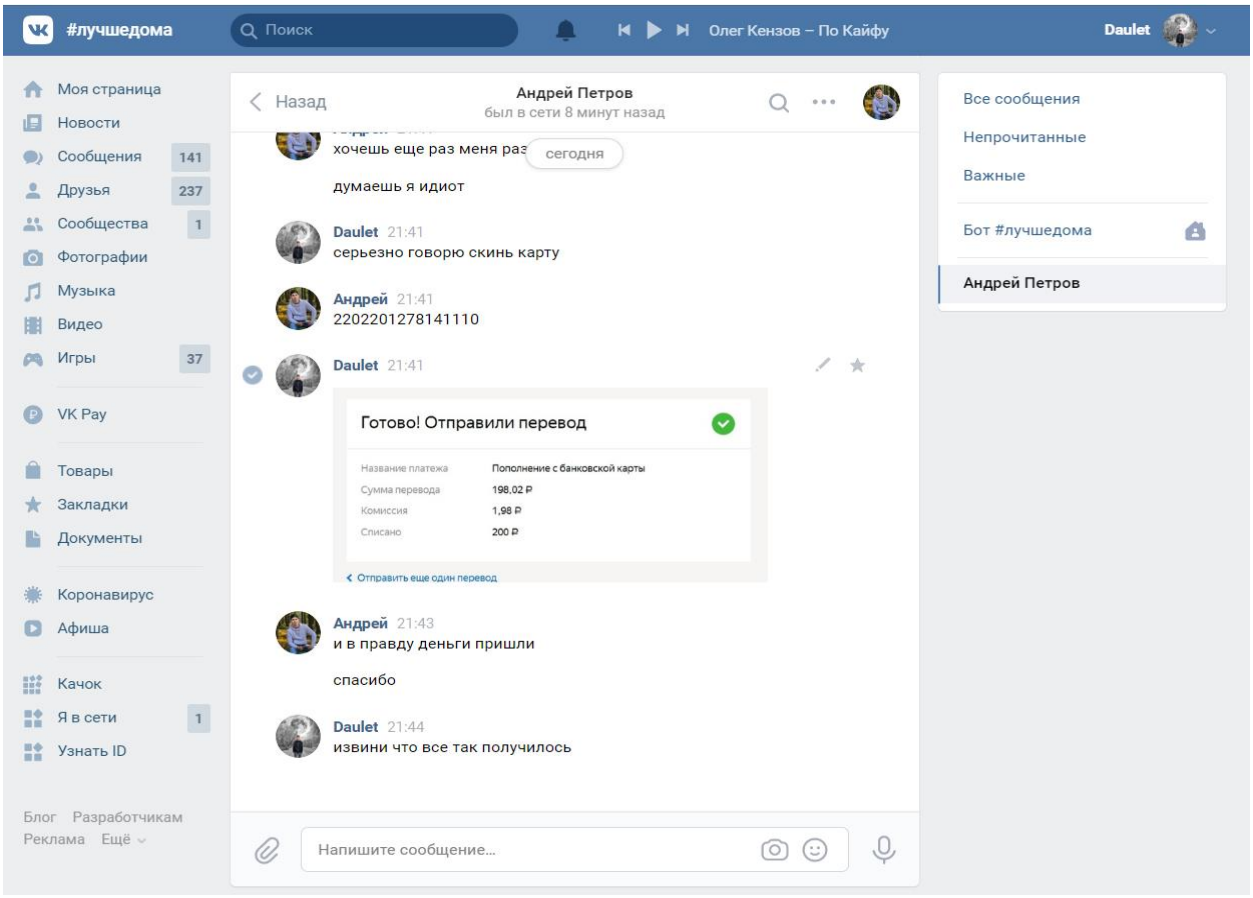
2.2 сурет – Нысанды бопсалау



3.19 сурет – Төлем алынғанның нәтижесі

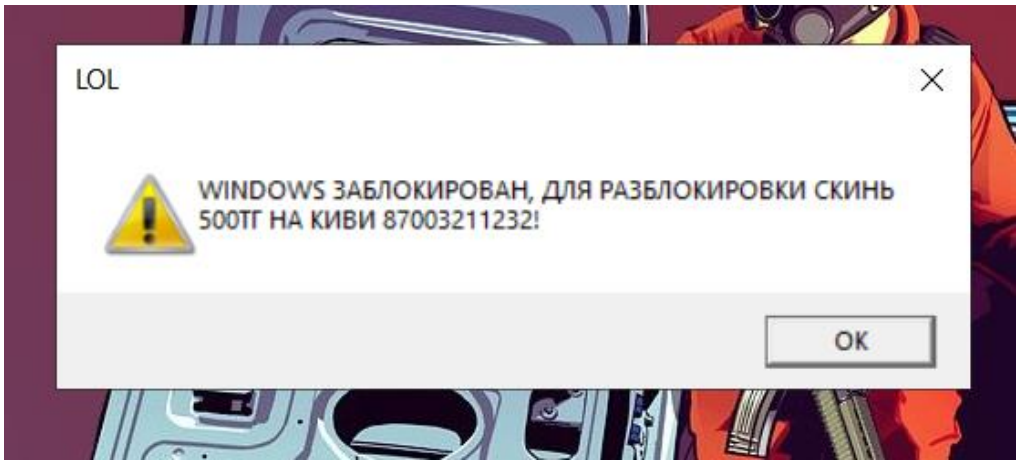


3.20 сурет – Төлем алынғанның нәтижесі

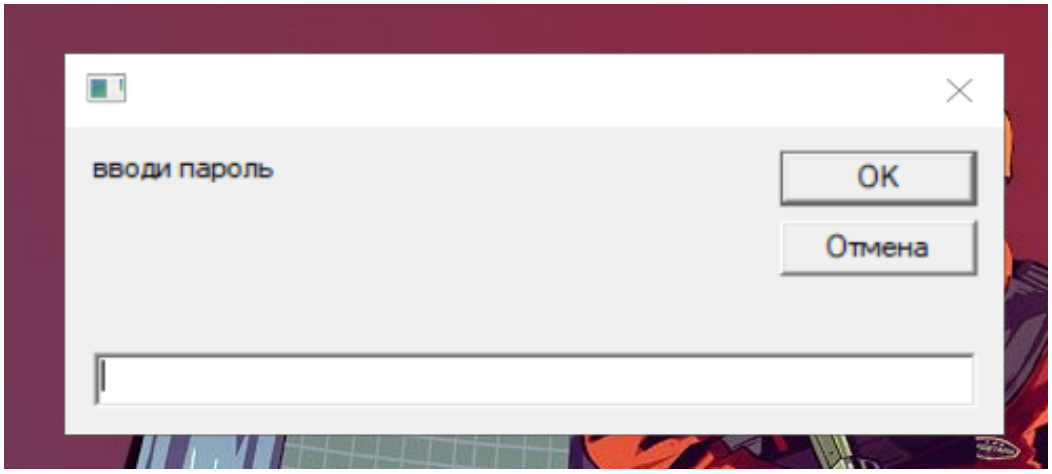


3.21 сурет – Жұмыс қорытындысы

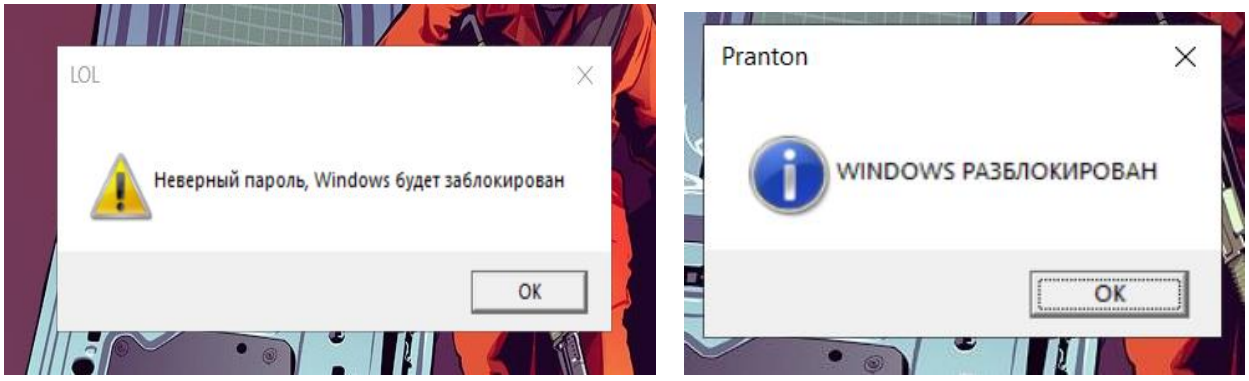
Бұл хабарлманы нысан жабу батырмаларын басқан кезде де, компьютерін өшіріп қайта қосқанда да, экран бетінен жоғалмайтын болады. Тек біз белгілеген құпия сөзді енгізген жағдайда ғана жойылатын болады. ОК батырмасын басқан кезде құпия сөзді енгізу терезесі шығады.



3.22 сурет – Бұғаттау хабарламасы



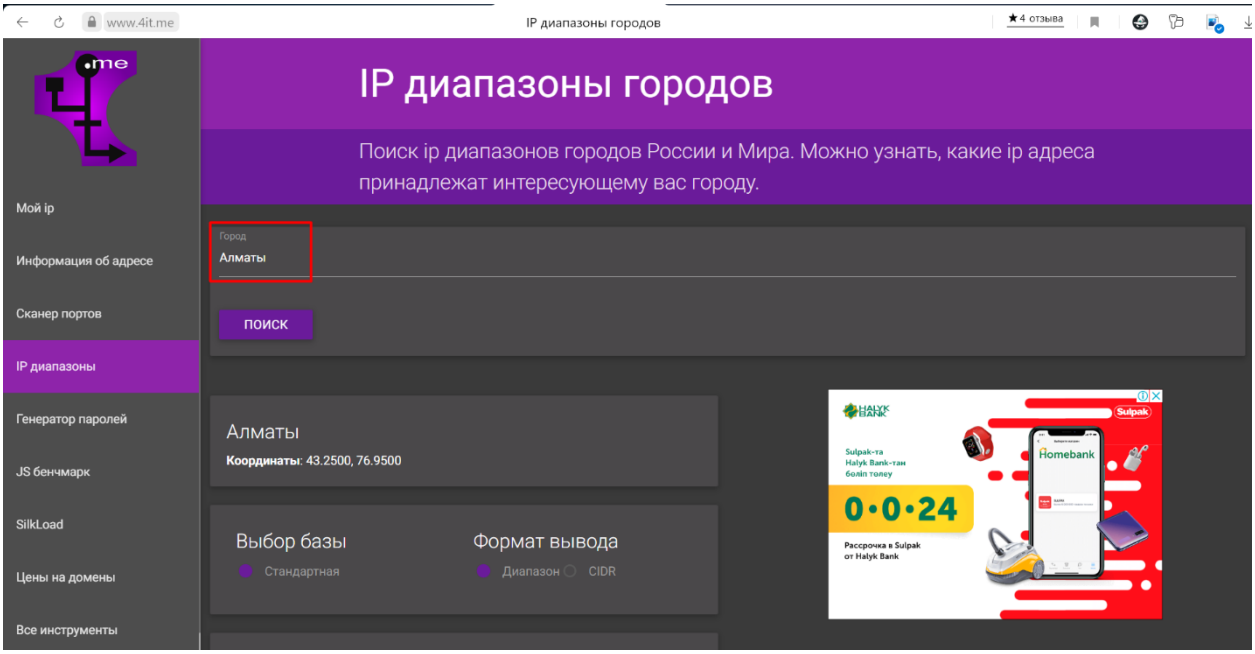
3.23 сурет – Құпия сөзді сұрау



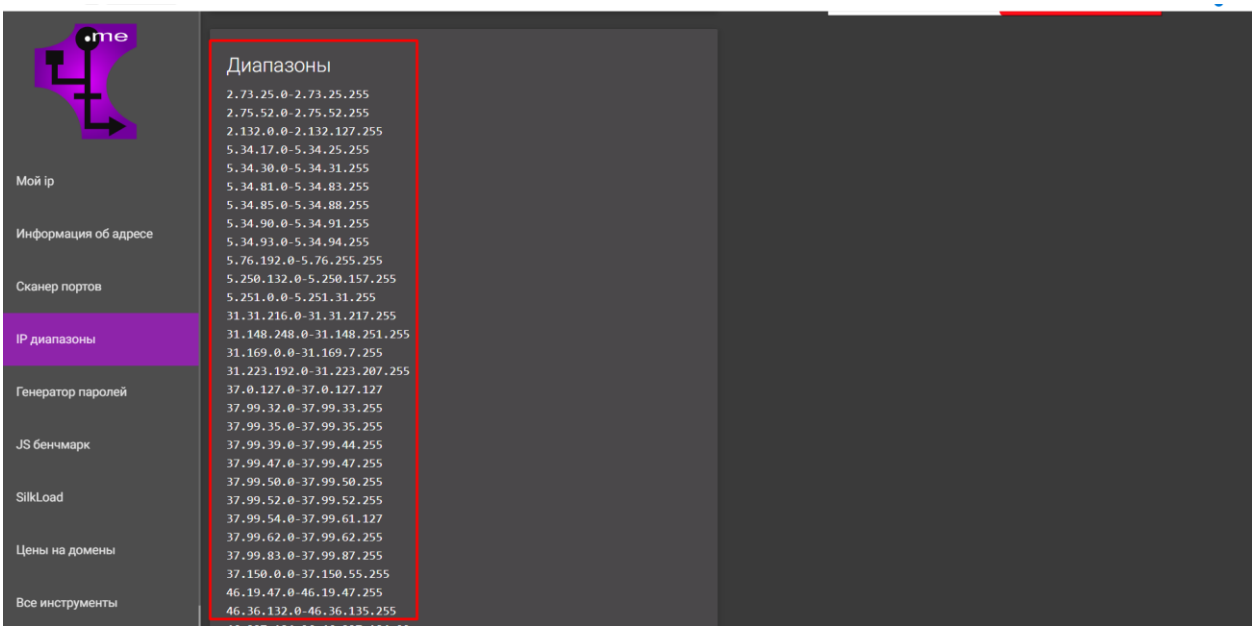
3.24 сурет – Құпия сөзді қате және дұрыс енгізудің нәтижелері

3.4 Әлеуметтік инженерияның төртінші тәсілі – бейнебақылау жүйелеріне шабуыл

Бізге керекті нысанның мекен-жайын енгізу бойынша IP-адрестердің диапазонын анықтаймыз.

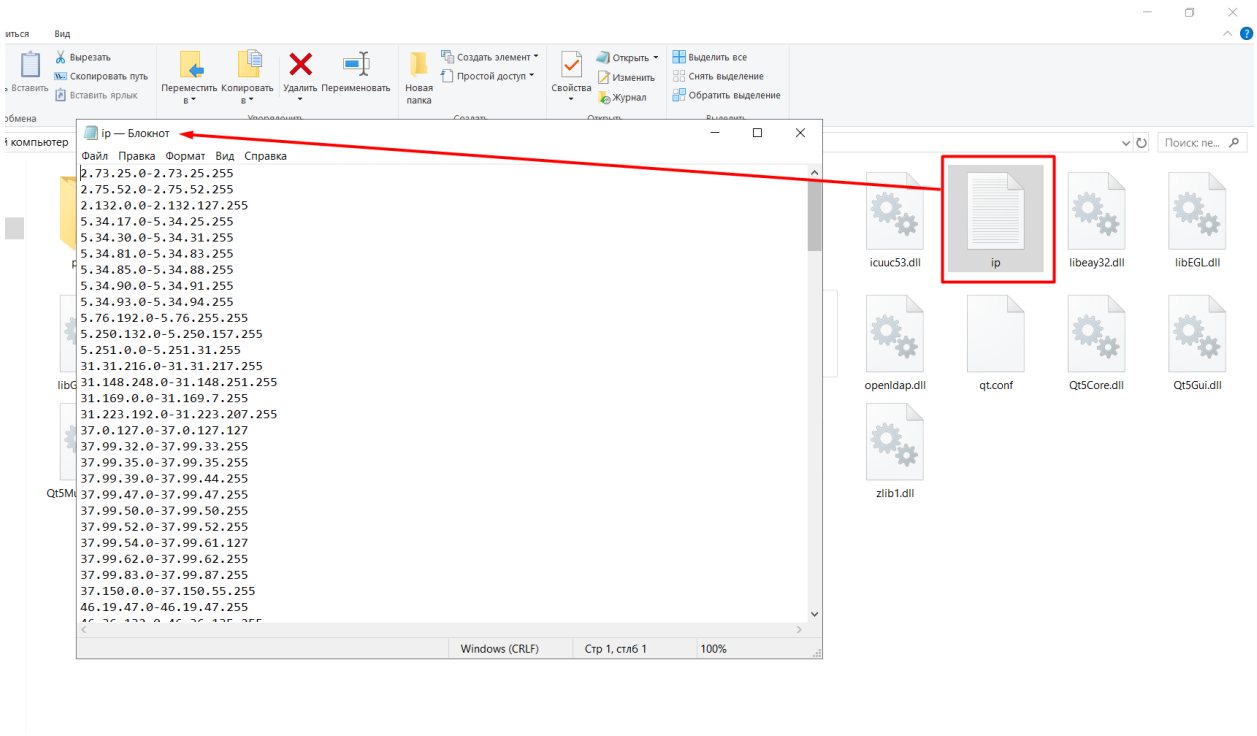


3.25 сурет – Мекен-жайды анықтау



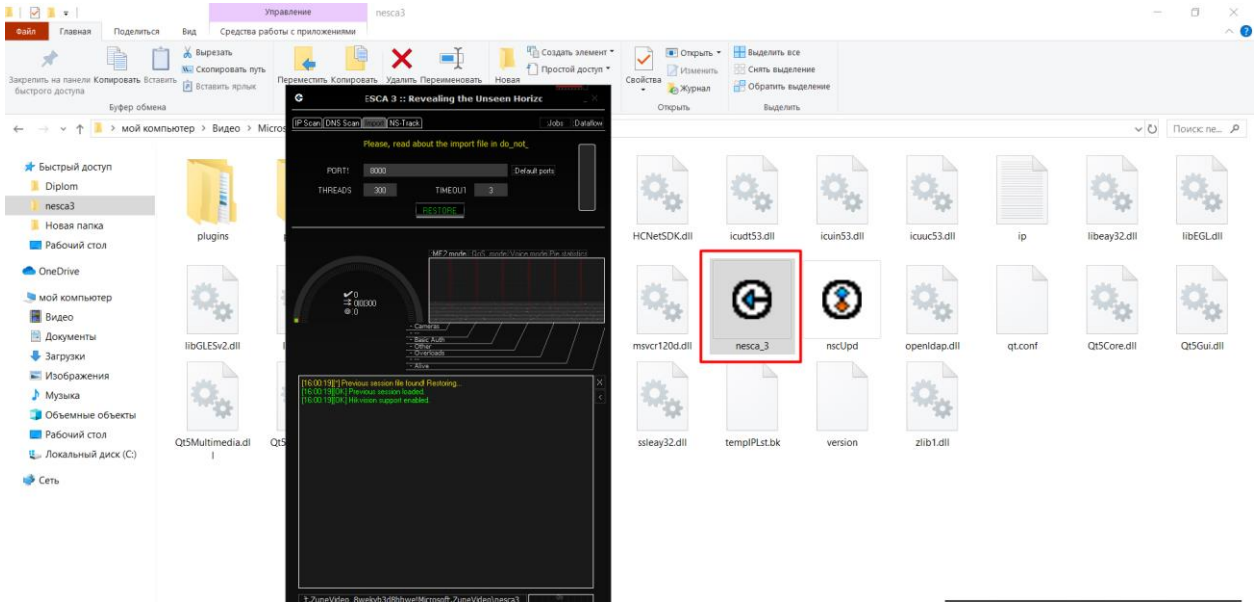
3.25 сурет – IP-адрестер диапазоны

Анықталған IP-адрестерді мәтіндік құжат ретінде сақтаймыз.

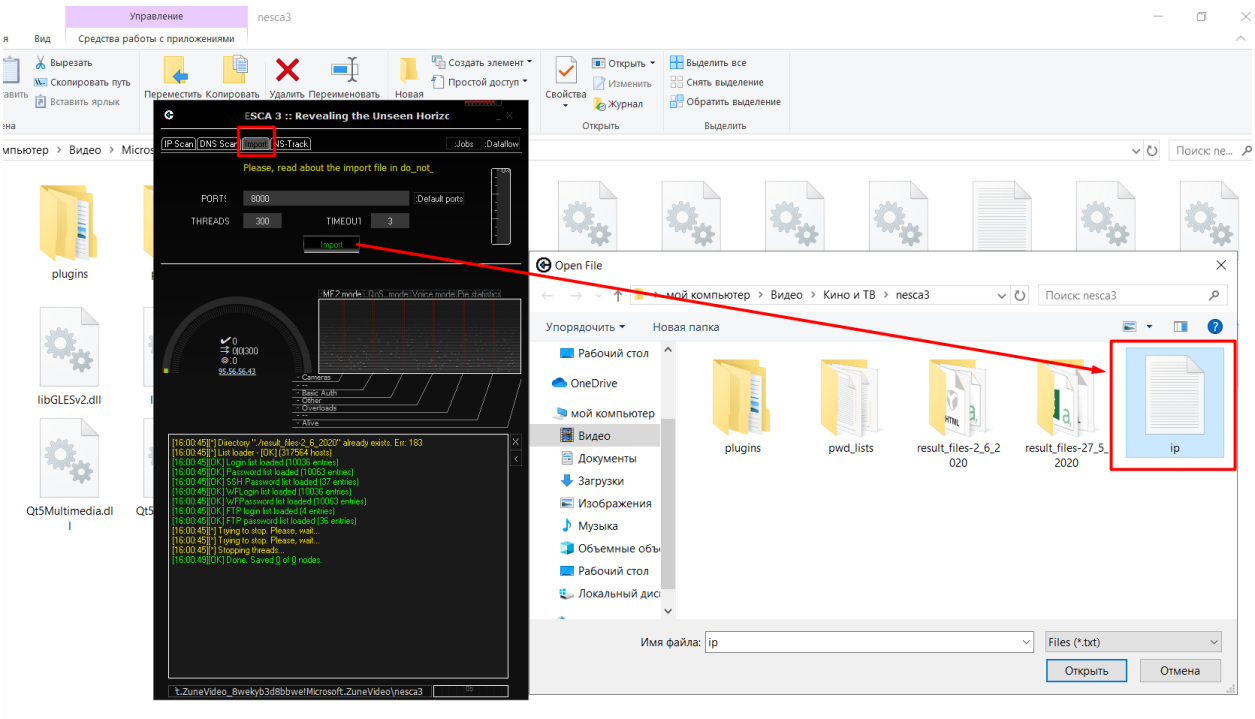


3.26 сурет – Мәліметтерді сақтау

Келесіде «NESCA-3» бағдарламасын қолданамыз. Мұнда мәтіндік құжатты импорттаймыз.



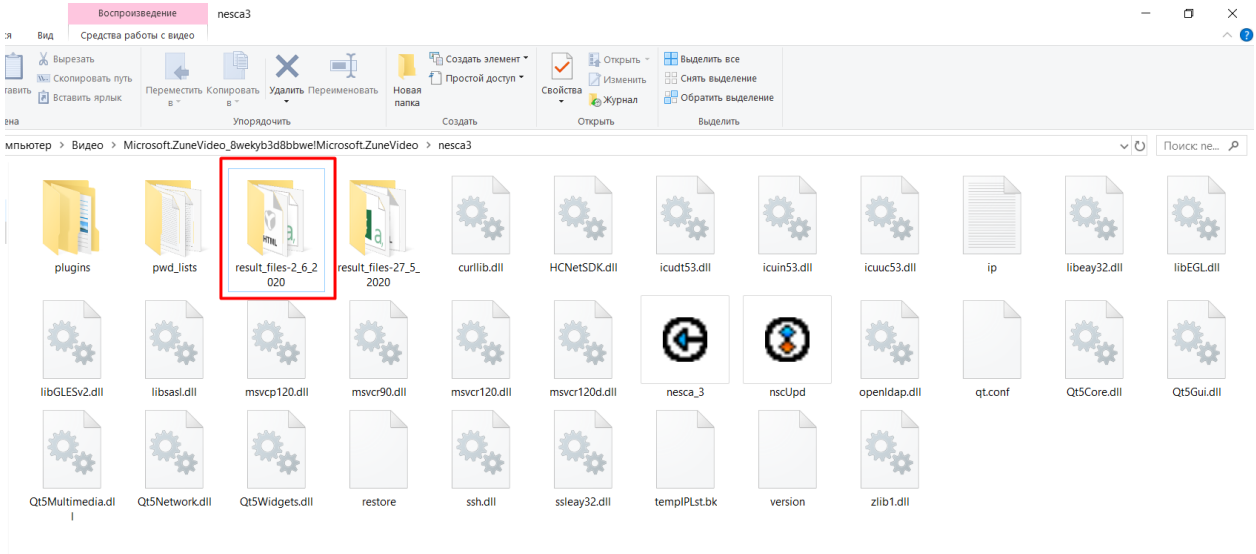
3.27 сурет – «NESCA-3» бағдарламасы



3.27 сурет – Құжатты импорттау

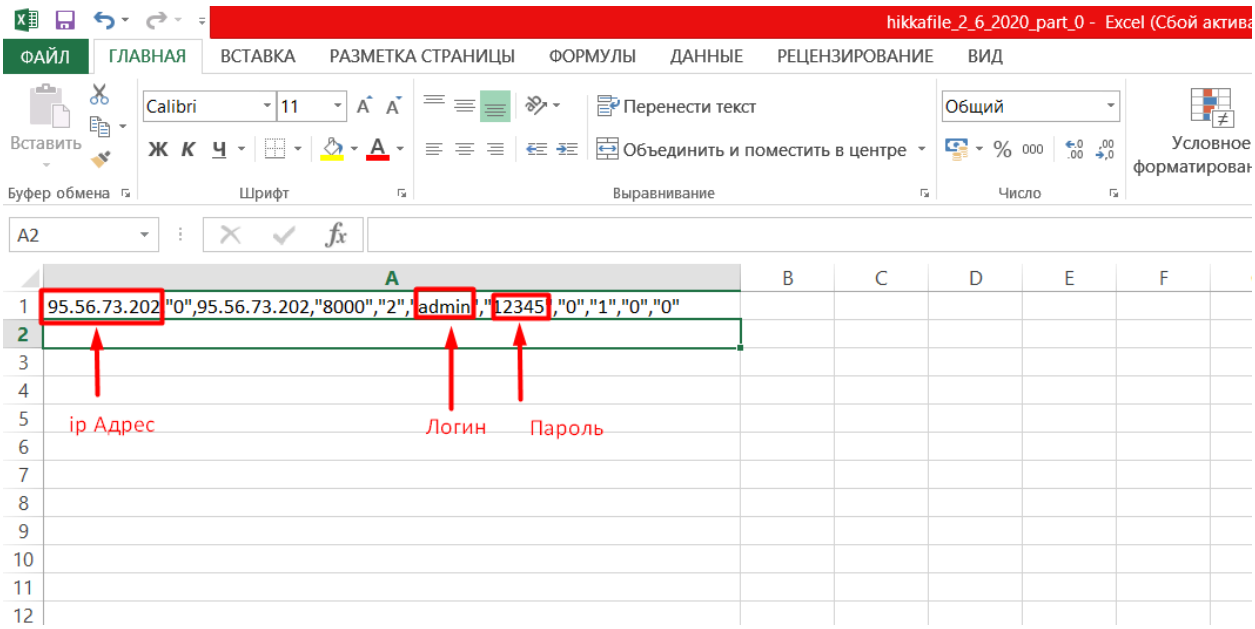
IP-адрестердің диапазонында кездейсоқ құпия сөздерді таңдау арқылы нысанның жеке деректеріне қол жеткіздік.

3.28 сурет – Құпия сөздерді таңдаудың сәтті нәтижесі



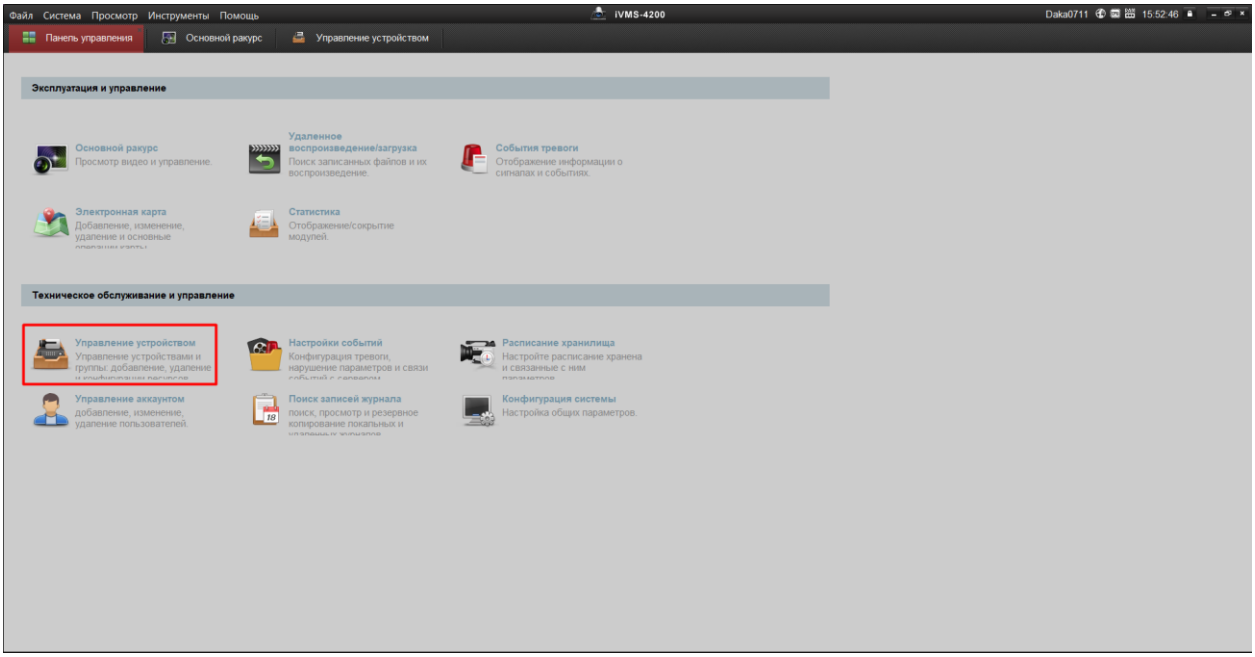
4.29 сурет – Мәліметтерді сақтау

Мәліметтер excel форматында сақталды, мұнда IP-адрес, логин және құпия сөз көрсетіледі.

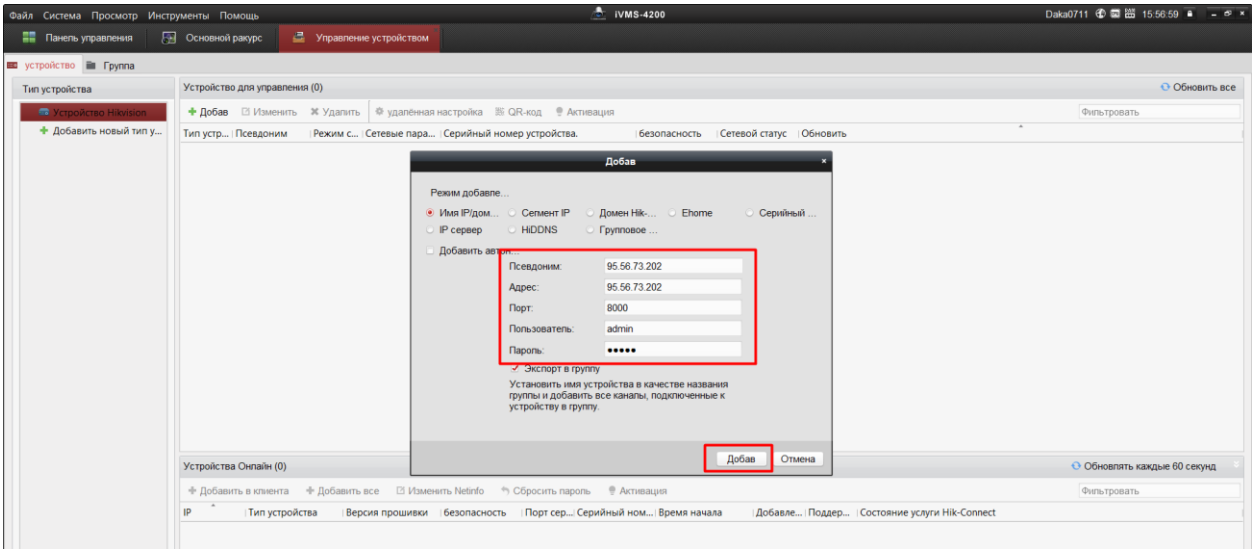


3.30 сурет – Мәліметтерді сақтау

Келесі қадамда бейнебақылау камераларын басқаруға арналған iVMS 4200 бағдарламасында сақталған мәліметтерді пайдаланып видеокамераны іске қосамыз.

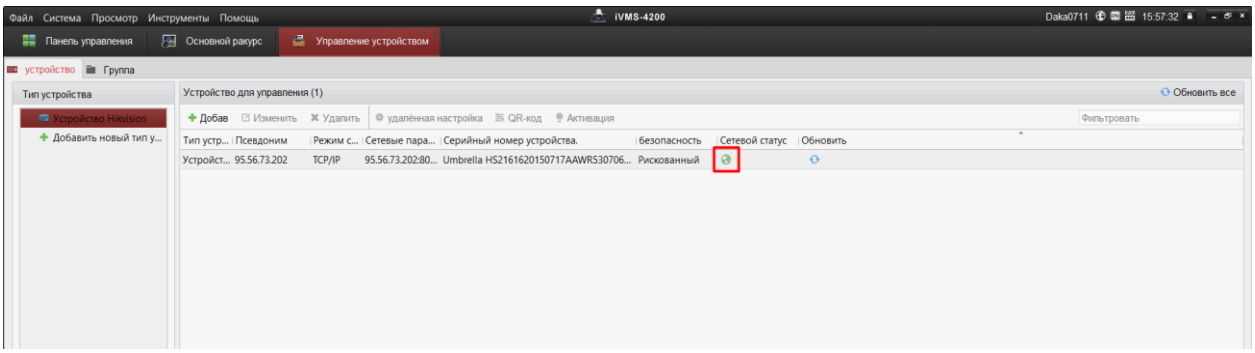


3.31 сурет – Бейнебақылауды басқару

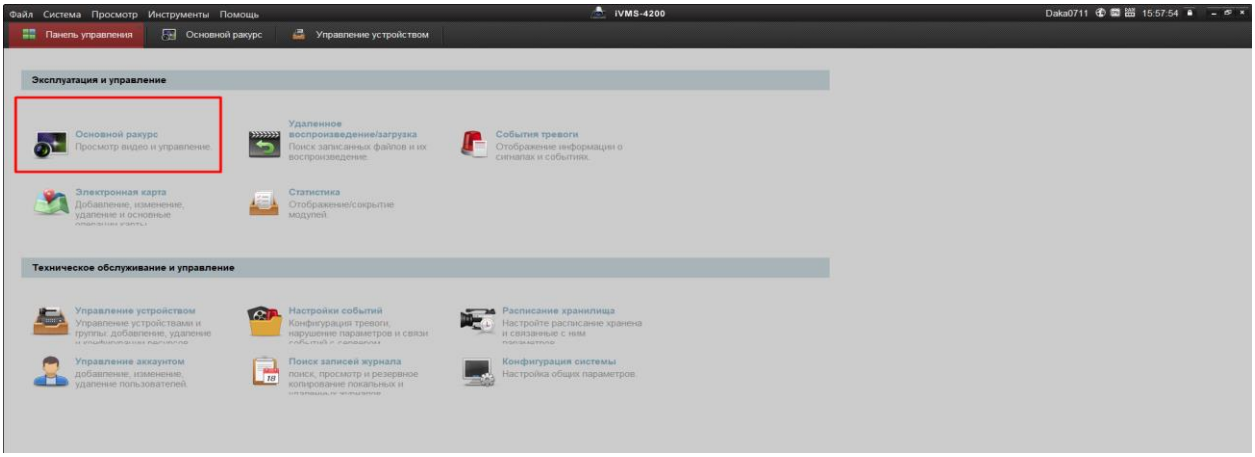


3.32 сурет – Жеке мәліметтерді енгізу

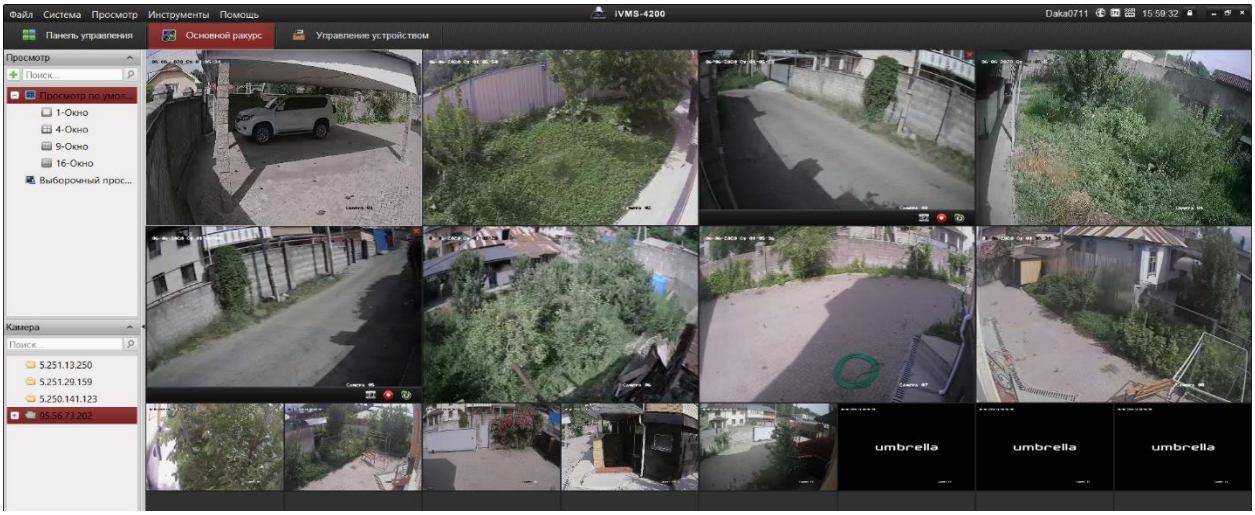
Жеке деректер сәйкес келген кезде видокамера өзінің желілік статусын өзгертеді және бақылауға мүмкіндік береді.



3.33 сурет – Қосылу процесі



3.34 сурет – Видеокамераны қосу



3.35 сурет – Бейнебақылауды басқару нәтижесі

Қорытындылай келе, жоғарыдағы қадамдарды орындап, нысанға бейнебақылау жүргізілді.

3.5 Әлеуметтік инженериядан қорғану немесе алдын алу жолдары

Компаниялардың компьютерлік жүйелерінің осалдылығын зерттейтін орындар, компьютерлік жүйелерге әлеуметтік инженерия арқылы кіру әдістері әр дайым 100% болғанын айтады. Ақпаратты қорғау технологиялары бұл әдісті қиындата түседі. Бірақ әлеуметтік инженерия мәселесін шешу үшін немесе алдын алу үшін ақпараттың қауіпсіздік технологияларымен, ақпаратты қорғау саясатының бірігуі керек. Ақпаратты қорғау саясатында жұмыскерлер өздерін қалай ұстау керек екені тұралы жазылуы тиіс. Сонымен қатар саясатта жұмыскерлерді дайындау тұралы ақпарат болуы тиіс.

Әлеуметтік инженериядан қорғанудың негізгі түрі болып жұмыскерлерді дайындау болып табылады. Барлық жұмыскерлер өздерінің немесе компанияның деректері кез келген уақытта сырт көзге ағып кетуі мүмкін екенін және ол зиянкестерден қалай қорғану керек екенін білу керек. Одан орай әр қызметкерлерде, жұмыс орнына және лауазымына байланысты қандай тақырыптарға қалай сөйлесу керек екені тұралы нұсқаулар болуы тиіс. Нұсқауда жұмыскер қандай ақпаратты техникалық қызмет көрсету орталығының жұмыскеріне беруге болады және компания жұмыскеріне өзіне керек ақпарат алу үшін қандай деректерді беру керек екені жазылуы тиіс. Қоғамдық инженерлер шабуылдарды жұмыскерлердің шынайылығына, еріншектілігіне, адамгершілігіне сүйене жасайды. Бұл шабуылдардан қорғану қиын, себебі жұмыскерлер зиянкес оны алдағысы келіп тұрғанын түсінбейді. Қоғамдық инженерлер, қарапайым зиянкестер секілді ақша, құпия ақпарат немесе компанияның IT ресурстарын алуға көздейді. Бұл шабыулдардан қорғану үшін, алаяқтықтың түр түрін зерттеу керек, зиянкеске қандай ақпарат керек екенін

түсіну керек, оны зерттеу керек. Зиянкес ісін жүзеге асырса, шығын қанша болатынын білу керек. Бұл ақпараттардың бәрін білсе, қауіпсіздік саясатына өзгертулер енгізіп, компанияны қорғауға болады.

- ақпаратты анализден өткізу – ақпаратты толығымен анализдеу керек;
- құпия болып келетін ақпаратты идентификациялау және оны әлеуметтік инженерияға осалдылығын тексеру. Құпия ақпаратты қауіпсіздік жүйелері сәтсіздікке ұшыраған кезде зерттеу;
- хатамалар құру – ақпаратты өңдеу, сақтау тұралы қауіпсіздік саясатын және протоколдарды құру;
- Event Test – уақыттан тыс қауіпсіздік тесттерін өткізу;
- қалдықтармен басқару – қоқыс қораптарына тек құпия емес ақпаратты тастау керек. Қоқыс кораптары құлыптармен құлталуы тиіс. Құлыптардың кілттері тек тазалау жұмыскерлерінде болуы тиіс. Қоқыстардың тұрған орындары айқындалуы тиіс, яғни зиянкес қоқыстан құпия ақпаратты алғысы келетін жағдайда қоқыс қорабынын тұрған орны үлкен рөл атқарады. Мысалы, қорап офис ортасында тұрған жағдайда, оған қол жеткізу қиын болып табылады, себебі адамдарда сұрақтар пайда болуы мүмкін.

Осыған орай, келесі ережелерді бөліп көрсетуге болады:

- қызметкерлердің кіретін идентификаторлары компанияның меншігі болып табылады. Барлық қызметкерлерге жұмыс орнынан берілген логин және құпия сөздер компания меншігі екенін және оны басқа мақсатта қолдануға (жеке пошта үшін, web парақшаларға кіруге және т.б.) болмайтынын немесе оны үшінші жаққа берілмеу керек екені айқын түсіндірілу керек. Мысалға, кейбір жұмыскерлер демалысқа ыққан кезде өзінің идентификаиорларын әріптесіне қалдырып кетеді;
- қызметкерлерге жиі қауіпсіздік шараларын ұлғайту мақсатында қауіпсіздік саясаты оқылуы керек. Бұндай шараларды өткізу, компания қызметкерлеріне актуалді қоғамдық инженерия әдістерін біліп жүруіне алып келеді. Қоғамдық инженерия әдісін білді деген сөз, шабуылдан 50 пайызға қорғану деген сөз;
- қызметкерлердің қол астында қауіпсіздік ережелер және нұсқаулықтар болуы тиіс. Нұсқаулықтарда жұмыскер әртүрлі жағдайлар туындаған кезде, не істеу керек екені жазылу тиіс. Мысалы нұсқаулықта, үшінші адам құпия ақпаратты сұраған кезде не істеу немесе қай жерге хабарласу керек екені тұралы ақпарат жазылуы мүмкін. Бұндай шаралар, ақпараттың ағып кетуінен сақтауға көмектеседі;
- қызметкерлердің компьютерлерінде актуальді антивирустық бағдарламалар болуы тиіс. Қызметкерлердің компьютерлеріне одан орай брэндмауерлер орнату қажет;
- компанияның корпоративтік жүйесінде қауіптілікті анықтау және шешу

жүйелері болуы керек. Құпия ақпараттардың ағып кетпеуін қадағалайтын жүйелер орнату қажет. Бұның бәрі фитиновтық шабуылдардаң қорғайды;

- барлық қызметкерлер келген клиенттермен қалай сөйлесу керек екені туралы ақпарат алуы тиіс. Келген кісінің кім екенің анықтаудың нақты ережелері болуы тиіс. Келген кісілердің қасында әр дайым компания қызметкерлері жүруі тиіс. Егер қызметкер компания ішінен бөтен кісіні көрсе, ережелер бойынша қызығушылық таныту керек. Кісі бұл жерде қандай мақсатпен жүр екенін және оның қасындағы компания жұмыскері қайда деген сұрақтар қойылуы тиіс. Қажет жағдайда қызметкер, бөтен адам тұралы ақпаратты қаіпсіздік қызметкерлеріне айтуы керек;
- барынша қызметкерлердің жүйедегі хақыларын азайту керек. Мысалы, қызметкерлерге web парақшаларына кіруді бөгеу және сыртқы ташығыштарды қолдануға рұқсат бермеу керек. Себебі, қызметкер ғаламтор желісінен фишингтік парақшаларды ұстамаса және сыртқы тасығыштар арқылы трояндық вирустарды компьютерге тасымаса, өзінің идентификаторларын жоғалту ықтималдылығы күрт түседі. Үстідегі бүкіл ережелерге сүйенсек ең мықты қорғаныс, ол жұмыскерлерді үйрету болып табылады. Әр жұмыскер, ережені бұзу жауапкершіліктен босатпайтынын білуі қажет. Әр қызметкер жеке ақпараттарының ағып кету қауіпін білу керек және оған қалай қарсы тұру керек екенің білу керек, себебі жүйенің ең осал бөлігі ол адам.

Келесіде қоғамдық инженерлердің амалдары жазылған:

- өзін басқа қызметкер ретінде немесе жаңа қызметкер түрінде таныстырып, көмек сұрау;
- өзін тасымалдаушы компанияның қызметкері немесе әріптес компания қызметкері ретінде таныстыру;
- өзін басқарушылардың бірі ретінде таныстыру;
- өзін қауіпсіздік бағдарламалардың немесе компанияға сай бағдарламалардың жұмыскері ретінде таныстырып, жаңартуларды орнату мақсатымен хабарласу;
- өзін техникалық қызмет көрсету орталығының қызметкері ретінде таныстырып, көмек көрсету және алдын ала шығатын қателерді енгізу. Қателердің енгізу себебі, сол қателерді түзеп сенімге кіру;
- сенімге кіру мақсатында компания ішіндегі таныс сөздерді, терминдерді қолдану;
- вирустарды немесе трояндық жылқыларды хабарландыруға қоса жіберу;
- жалған pop-up терезесін жіберу. Бұл терезе идентификаторларын қайта теруге өтініш білдіреді;
- парақшаға тіркелсеніз ұтыс аласыз деген жалған хаттар жіберу;
- жұмыскер басып отырған батырмаларды өз компьютеріне немесе кейлогинггбағдарламасына жазу;

- сыртқы тасымалдағыштарды көзге көрінетін жерлерде тастап кету;
- құжаттарды немесе папкаларды компанияның пошта бөліміне тастап кету;
- құжатты локальді адреске жіберуді өтіну;
- шабуылдаушы өзінің дауысын өзгерту, жұмыскер оны өз әріптесі деп ойлау үшін.

Қауіптердің түрлері және алдын алу іс-шаралары:

- телефонмен байланысты қауіптер. Телефон қазіргі күнге дейін компания ішінде немесе компания аралық коммуникация түрі болып табылады және қоғамдық инженерлерде көп қолданысқа ие. Телефон арқылы адамның түрін көре алмаудың себебінен, зиянкес өзін әріптес, бастық немесе конфиденциалды ақпаратқа қолы жетімді кез келген адам ретінде өзін таныстыра алады. Зиянкес, көбінесе өз өтінішін жұмыскер орындауға тиіс болатындай сұрайды, әсіресе өтініші оңай көрінгенде. Телефон арқылы ақша ұрлаудың басқа да түрлері әйгілі. Ұтысты қайта қайтару, конкурстан жеңіңпаз атану немесе жақын адамдардың келеңсіз жағдайға түсіп, тез арада ақша сұрау тұралы смс немесе қоңырау келуі мүмкін. Қауіпсіздікті сақтау шаралары бұндай смс-терге скептикалық көз қараспен қарауды ұсынады және келесі принциптерді ұстануға шақырады. Хабарласып тұрған адамның тұлғасын тексеру. Нөмерді анықтау қызметтерімен қолдану. СМС- тегі таныс емес сілтемелерді елемеу.
- электронды пошта арқылы келетін қауіп қатерлер. Көптеген қызметкерлерге күн сайын корпоративтік немесе өздерінің электронды пошталарына, күн сайын он немесе жүздеген хабарландырулар келеді. Әрине бұндай ауқымдағы хаттардың бәріне тиісті көңіл аудару мүмкін емес. Бұл шабуылды жасауға үлкен көмек. Көптеген жүйенің пайдаланушылары бұндай хабарландыруларды өңдеуде қауіпті ешнәрсе көрмейді. Пайдаланушылар бұны құжаттарды бірінші папкадан екінші папкаға ауыстырудың электронды аналогы деп көреді. Зиянкес пайдаланушыға оңай сұрау жіберген кезде, пайдаланушы ойланбастан сұрауды жүзеге асырады, себебі сұраудан ешқандай қауіп көрмейді. Хабарландыруларда сілтемелер болуы мүмкін. Сілтемелер, пайдаланушы компанияның құпия ақпаратын жарыққа шығаратын іс-қимылдар жасайды. Көптеген қауіпсіздік жүйелері, авторизациядан өтпеген пайдаланушылар корпартивтік жүйеге кірмеуін бақылайды. Егер пайдаланушы, зиянкес жіберген сілтеме бастырмасын басса, корпаративтік жүйеге трояндық вирусын кіргізеді. Вирус, компанияның көптеген қауіпсіздік жүйелерінен өтіп кетуге мүмкіндік алады. Қалған қауіптер секілді, электронды поштаны қорғау үшін, келген хабарландыруларға скептикалық тұрғыдан қарау керек. Бұл тұрғыдан қарау үшін, қауіпсіздік саясатына бірнеше өзгертулер еңгізу керек.

Бұл енгізулер тізімі көрсетілген:

- құжаттарға қосылып келген тіркемелер;

- құжаттардағы сілтемелер;
- компанияның ішінен келген хатта, жеке немесе корпоративтік ақпараттар сұралса;
- компанияның сыртынаң келген хатта, жеке немесе корпоративтік ақпараттар сұралса;
- бір сәтте хабарландырулармен ауысуға арналған қызметтерді қолдану кезіндегі қауіптер. Бір сәтте хаттармен ауысу қызметі жаңа әдіс болып саналғанмен, қазіргі кезде корпоративтік пайдаланушылар арасында әйгілі болып кетті. Бұл әдістің тездігі және оңайлығы, зиянкестердің шабуылына үлкен мүмкіндіктер береді. Пайдаланушы бұл қызметті, телефондық жүйе ретінде көріп, қауіпті бағдарламалармен байланыстырмайды. Сондықтан бұл әдіс қауіпті болып табылады [12].

4 Өміртіршілік қауіпсіздігі

4.1 Жұмыс жағдайын талдау

Дипломдық жұмыстың мақсаты әлеуметтік инженерияның зардап шеккен адамға әсер ету әдістерін талдай келе, осалдықтарға қарсы іс-қимыл әдістемесін әзірлеу.

Өміртіршілік қауіпсіздігі бөлімінде табиғи жарықтандыруды, өрт қауіпсіздігін және хабарлағаш санын есептеу туралы шешім қабылданды.

Өндірістік бөлмеде (операторлық) бес дербес компьютер орналасқан және олар RJ-45 кабелі арқылы ғаламторға байланысқан.

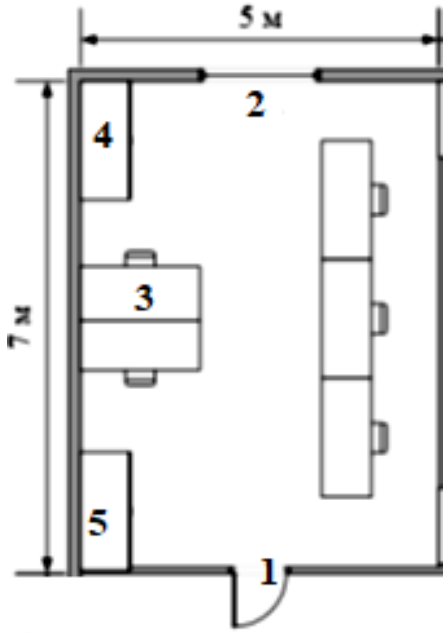
Бөлмеде бес жұмыс орнын ұйымдастарылған (бір жетекші инженер және төрт кезекші оператор). Жетекші инженердің бес күндік жұмыс уақыты 8 сағаттан. Ал төрт кезекші операторлар ауысыммен ауысып жұмыс істейді. Жұмыс уақытынан тыс тамақтануға және тынығуға арналған 60 минуттық үзіліс уақыты бар [13].

Өрт қауіпсіздігі мәселелері бойынша жұмыс бөлмесі «D» санатына жатады. Өрт қауіпсіздігінің стандартты ережелеріне сәйкес, әкімшілік ғимараттар мен жеке бөлмелер, технологиялық қондырғылар ережелерге сәйкес бастапқы өрт сөндіру құралдарымен қамтамасыз етілген [14].

Жұмыс бөлмесінің параметрлері:

- бөлме өлшемдері: ауданы 35 $м^2$, ұзындығы 7 м, ені 5 м, биіктігі 3 м;
- терезенің өлшемі:1,5 м*1,2 м;
- бөлмеде екі қатарда алты жұмыс үстелі орналасқан, онда пульттер, қайта таратқыштар орнатылған;
- үстелдің ұзындығы 90 см, ені 60 см, үстелдер арасындағы өткелдер ұзындығы 1,5м, үстелдер қабырғадан 0,5 м қашықтықта орналасқан;
- жұмыс санаты жеңіл физикалық, Іа санаты, жұмыс отыру күйінде өтеді (адам организмінің энергия шығыны – 138-172 Ккал/сағ)

4.1-суретте бөлменің жоспары көрсетілген, онда 1 − есік, 2 − терезе, 3 − жұмыс үстелі, 4 –салқындатқыш, 5 – шкаф.



4.1 сурет – Бөлменің жоспары

Операторлардың шаршауы мен күш салуын арттырмау үшін өнеркәсіптік комфорт жағдайын ұйымдастырамыз және жұмыс компьютерде ұзақ тұрумен байланысты болғандықтан, қолайлы жұмыс жағдайларын қамтамасыз ету үшін жарықтандыру жүйесін қарастырамыз.

4.1.1 Жұмыс орынын ұйымдастыру

Эргономикалық талаптарды ескере отырып қызметкердің жұмыс орындарын ұйымдастыру барысында жұмыс орнының конструкциясы және оның барлық элементтерінің өзара орналасуы антропометриялық, физикалық және психологиялық факторлары ГОСТ 50923-96 [15] талаптарын басшылыққа аламыз.

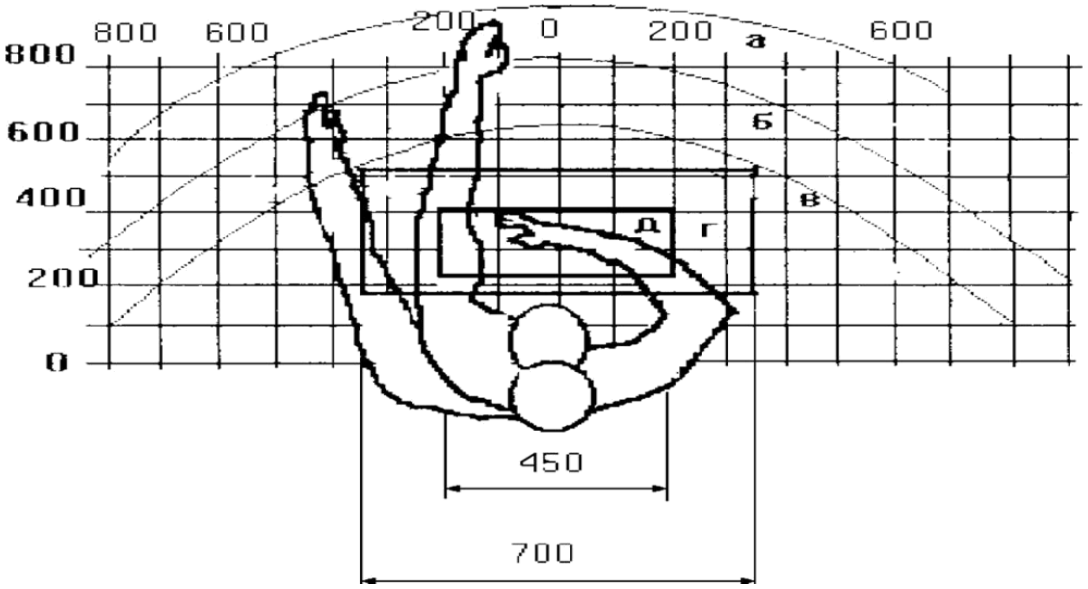
Осы ретте жұмыс істеу ортасы мен еңбек процесінен зиянды және қауіпті факторлар болады:

- көру мен зейінге күш түсіру;
- қол, арқа, мойын омыртқаларына статикалық және динамикалық күш түсуі, жұмыстың жоғары қарқыны;
- жоғары жүйке-психикалық, эмоциялық және зияткерлік күш түсуі;
- еңбек және демалыс режимін бұзу;
- тиімсіз жұмыс орнын ұйымдастыру
- қуатты көздерден магнит өрісінің әсерінен жұмыс орнындағы дисплейдің көрнекі параметрлерінің нашарлауы;
- дисплей экранындағы бейненің пиксельділігі: дисплей экраны сәулелерінің табиғи жарық спектріне сәйкес келмеуі; экраннан көрінетін жарықтың артық ағындары (әсіресе көк-күлгін жарық) және т.б.

Жұмыс орнын ұтымды жоспарлау заттарды, еңбек құралдарын және құжаттаманы орналастырудың нақты тәртібі мен тұрақтылығын көздейді. Жұмысты орындау үшін талап етілетін нәрсе жұмыс кеңістігінің жеңіл қол жеткізу аймағында орналасады.

Жұмыс орнының параметрлері антропометриялық сипаттамаларға сәйкес таңдалады. Бұл деректерді есептерде пайдалану кезінде ең жоғары антропометриялық сипаттамалардан (М+2) алынады.

Оператордың жұмыс орны 4.2-суретте көрсетілген, онда а - қолдың максималды жету аймағы, b - алақанмен саусақтардың жету аймағы, с - алақанға оңай қол жеткізу аймағы, d - қолмен жұмыс жасау үшін оңтайлы кеңістік, d - қолмен жұмыс жасау үшін оңтайлы кеңістік.



4.2-сурет – Оператордың жұмыс орны

Жұмыс үстелін құру кезінде келесілерді ескертулерді сақтаңыз:

- үстелдің биіктігі ыңғайлы жерде отыру ықтималдығын қамтамасыз етеді, қажет болған жағдайда тіректерге сүйенуге болады;
- үстелдің төменгі жағы оператордың аяғын қыспастан ыңғайлы құрастырылады;
- үстелдің беті қызметкердің көру радиусында жарқыл мен шағылыстың пайда болуынан әсер етпейді;
- үстел құрылғысы жылжымалы жәшіктер болады (құжаттарды, кеңсе қағаздарын, жеке пайдалану заттарын сақтау үшін кемінде 3 жәшік).

Бағдарламашы жұмыс орнының маңызды құрамдас бөлігі – орындық. Ол ГОСТ 50923-96 [15] бойынша орындалады. Орындықты жобалау кезінде оператордың кез келген жұмыс жағдайында оның позасы физиологиялық дұрыс негізделінеді, яғни дене бөліктерінің орналасуы оңтайлы болады.

Отырып жұмыс істеу кезінде орындық конструкциясы келесі негізгі талаптарды қанағаттандырады:

- дене корпусының және оның аяқ-қолдарының бір-біріне қатысты еркін қозғалуы;
- оператордың бойының өсуіне сәйкес биіктіктің өзгеруіне жол беру (400 мм-ден 550 мм-ге дейінгі аралықта);
- артқа жеңіл көлбеу болуы;

Жоғарыда айтылғандарды ескере отырып, оператор үстелінің параметрлерін келтіреміз:

- үстел биіктігі 710 мм;
- үстел ұзындығы 1300 мм;
- үстелдің ені 650 мм;

Жазу үшін үстелдің беті:

- 40 мм тереңдікте;
- ені 600 мм.

Монитор жұмыс үстелінде немесе тұғырықта орналастырылады, оның экранындағы ақпаратты бақылау қашықтығы оператордың көзінен 700 мм-ден аспайды. Әріптер мен сандар үшін ұсынылатын мәндер 15-18 мм. Монитордың экраны 20 градус бұрышта орналасады, биіктігі бойынша бұл бұрыш экран ортасы мен көздің көлденең сызық деңгейінде болады. Көлденең жазықтықта бұрыш экранды бақылау 60 градустан аспайды.

Осылайша жұмыс орнын дұрыс ұйымдастыра отырып, қызметкердің еңбек өнімділігін 8 % -дан 20%-ға дейін көтеруге болады.

4.1.2 Жарықтандыру жүйесі

Бөлменің жарықтандыру жүйесі жобалауы ҚР ҚНжЕ 2.04-05-2002 [16] нұсқаудағы қабылданған жалпы қағидаларға сай келеді.

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

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

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

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

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

Өндіріс бөлмелерінде жарықтанудың табиғи және жасанды түрлері қолданылады.

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

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

Дисплейі бар бөлмелерді жарықтандыру бірқатар талаптарға сәйкес жүзеге асырылады:

- жұмыс бетіндегі және қоршаған кеңістіктегі жарықтылық мүмкіндігінше біркелкі таралады;
- жарықтандыру дұрыс жарық беру үшін жарықтың қажетті спектрлік құрамын қамтамасыз етеді.
- қағаздар, құжаттар және пернетақта аймағында көлденең жазықтықта жарықтандырудың қажетті деңгейі қамтамасыз етіледі;
- экранның тік жазықтығында жарықтандыруды шектеу арқылы дисплейдегі суреттің жарықтандырылуынан сақтандырылады;
- жұмыс бетіндегі өткір көлеңкелер болмайды, олардың болуы жарықтықтың біркелкі таралуына кедергі тудырады;
- қызметкердің орталық көз өрісінде және периферия аймағында жарықты тиісті бөлу қамтамасыз етіледі;
- жұмыс орнындағы жарық СанПиН 2.2.4.548-96 [17] гигиеналық нормаларға сәйкес;
- жарықтандыру пульсациясының тереңдігі шектеледі.

4.1.3 Электр қауіпсіздігі негіздері

Қоғамдық ғимараттардың электр қауіпсіздігі Қазақстан ҚР ҚНжЕ 2.04-01-2001 [18] талаптарына сәйкес жобаланады.

Электр қауіпсіздігі талаптарына сәйкес электр қондырғылары мен желілері пайдаланылатын кернеуге сәйкес 1000 және 1000 В-қа дейін бөлінеді. Бұл бөлу 1000 В-тан жоғары кернеумен жабдықталған қондырғыларға техникалық қызмет көрсетуді талап етеді және оларға жоғары білікті мамандар қызмет көрсетеді.

Адамдарға әсер етудің негізгі себептері: кездейсоқ байланыс немесе тірі бөлшектерге қауіпті қашықтыққа жақындау; персоналдың оқшауланууына немесе қате әрекеттеріне нұқсан келтіру нәтижесінде жабдықтың металл бөліктеріндегі кернеудің пайда болуы.

Тоқ соғудан келесі қорғану шараларын ұстаныңыз:

- оқшаулау;
- ағымдық тасымалдау бөліктерінің қол жетімсіздігі;
- арнайы ажыратқыш трансформаторлар арқылы электр желісін бөлу;
- төмен кернеуді пайдалану (42 В жоғары емес және өте қауіпті үй-жайларда, 12 В);
- қосарлы (жұмыс және қосымша) оқшаулауды пайдалану;
- әлеуетті теңестіру;
- қорғаныс жерге тұйықтау және нөлге келтіру; қауіпсіздік өшіру; арнайы электрлік қорғаныс құралдарын пайдалану;
- электр қондырғыларын қауіпсіз пайдалануды ұйымдастыру.

4.1.4 Өрт қауіпсіздігі қойылатын жалпы талаптар

Өртке қарсы шараларға қойылатын талаптар ҚР ҚНжЕ 2.02-05-2009 [19] құрылыс проект нормаларына сай жасалынады. Электр тораптарына, соның ішінде электронды компьютерлерге қосылатын әртүрлі мақсаттағы құрылғылармен жұмыс істеу кезінде қадағаланды. Дұрыс жасалған құжат электрлік құрылғылармен жұмыс бөлмесінде сипаты дұрыс емес жағдайлардан туындайтын қауіпті жағдайларды болдырмауға көмектеседі.

Монитордан және жүйелік блоктан шығатын кабельдер, сондай-ақ CRT мониторларындағы жарық түтігі жұмыс істеп тұрған электр кернеумен жұмыс

істейді. Осы құрылғыларды абайлап, дәлме-дәл пайдалану шкафта өрттің пайда болуына немесе адамның электр тогына түсуіне себеп болады.

Осыдан жұмыс компьютерлік кабинетінде мінез-құлық ережелерін сақтаңыз:

- қосқыштарды, қуат сымдарын, жерге тұйықтау құрылғыларын, монитордың артқы жағына түртуге тыйым салынады; тек таза, құрғақ қолдармен электр құрылғылармен қолдану;
- жұмыс аймағына кірмеңіз;
- ақаулы түрі бар электр сым ашасын розеткаға салуға тыйым салынады;
- жұмыс үдерісі кезінде сымның қыздыру дәрежесін бақылау қажет;
- жабдықты өзіңіз жөндеуге болмайды;
- электр лампаларының бетіне қағаз, шүберек және басқа да жанғыш
- материалдарды қоюға тыйым салынады;
- жоғарғы қуатты электр құрылғыларын бір розеткада қосуға болмайды;
- егер құрылыс кодекстерімен көзделмесе, сыныпқа жиһаз және
- жабдықты қайта өңдеуді жүзеге асыруға тыйым салынады;

Егер ғимарат өртеле бастаған болса, қажет шаралар:

- барлық электронды жабдықты ажыратыңыз;
- өртті жою үшін сақтық шараларын қолданыңыз;
- мүмкіндігінше материалдық активтерді босату;
- тиісті қызметтерге өрт туралы есеп беру − кезекші, басқарушы

- бақылау пункті.

Егер электрлік кернеу ДК-ның металл бөліктерінде немесе жердегі сымдарда анықталса, жабдықты кешіктірусіз ажыратыңыз. Компьютерлік бөлмеде жұмыс істейтін адамдар электр тогынан зардап шегетін адамдар мен күйіктерден зардап шеккен адамдардың басымдықты шараларын біледі.

4.1.5 Хабарландыру жүйесі

Қоғамдық ғимараттардың өрт кезіндегі хабарлау жүйесі ҚР ҚН 2.02-11-2002 [20] талаптарына сәйкес орындалады.

Объектіде орнатылған күзет-өрт сигнализациясының қазіргі заманғы жүйесі арнайы құрылғылардың тұтас жиынтығынан тұратын техникалық кешен болып табылады. Олардың негізгі мақсаты-қауіп туралы алдын ала ескерту үшін жағдайды қамтамасыз ету.

Күзет – өрт сигнализациясының кешенді жүйелерін жобалау қондырғының бірінші кезеңін білдіреді және техникалық іс-шаралардың тұтас кешенін орындауды көздейді. Олардың сапасына өрт сөндіру және күзет дабылының жұмыс тиімділігі байланысты.

Орнату барысында жобаға сәйкес құбырларда (немесе арнайы қорғау гофрасында) төселуі тиіс кабельдер мен сымдардың қосымша қорғанысын қарастырылады.

Өрт сигнализациясының техникалық жобасын әзірлеу кезінде сондай-ақ элементтері бойынша әдетте жалғау желілерін (шлейф) орнату жүргізілетін осы объектінің конструкциясының ерекшеліктері ескеріледі. Ол үшін объектінің жоспарлануын мұқият зерттеу және келесі міндетті бөлімдерді қамтитын сараптамалық бағалау дайындалады:

- конструкцияның күрделілік деңгейі;
- қызметтік үй-жайлар мен бөлмелердің;
- жоспарлау ерекшеліктері.

Күзет өрт сигнализациясы аспаптан дабыл сигналы келіп түскен жағдайда, жалпы мақсаттағы трансляция үзіледі және өрт туралы хабарлау жүйесі жад блогына жазылған немесе диспетчер оқитын шұғыл хабарламаны бере бастайды.

Адамдарды өрт туралы уақытылы хабардар етуде келесі ережелерді сақтаңыз:

- өртті анықтаудың аз инерциялық құралдары қолданылады;
- өрт туындауы неғұрлым ықтимал бөлмелерде және жану өнімдерінің ықтимал таралу жолдарында өрт хабарлағыштарын орналастырылады;
- ЭҚЖ іске қосылуының барынша рұқсат етілген уақытын анықтау үшін ықтимал жағдайлар алдын ала талданады (өрт анықталған сәттен бастап хабарлау сигналдарын беруге дейін);
- ЭҚЖС құрылымдық схемасы әзірленеді және өрт қауіпсіздігі жүйесінің рұқсат етілген жұмыс істеу уақыты қолданылады.

- Адамдарды өрт туралы хабардар етуде келесі шараларды орындаңыз:

- адамдар өрттің қауіпті факторларының әсеріне ұшырауы мүмкін үй-жайларға, сондай-ақ эвакуациялық жолдарды өрт бұғаттаған кезде адамдар қалуы мүмкін үй-жайларда дыбыстық және жарық сигналдар беріледі;

- эвакуациялау қажеттілігі туралы, эвакуациялау жолдары және қауіпсіздікті қамтамасыз етуге бағытталған іс-қимылдар туралы сөйлеу түрінде ақпараттар таратылады.

4.2 Есептеулер

4.2.1 Жұмыс бөлмесінің табиғи жарықтандыру есебі

Есеп әдістемелік нұсқауды негізге ала отырып орындалды [21].

Табиғи жарық табиғи жарықтану коэффициентімен сипатталады (ТЖК). ТЖК – аспанның (тікелей немесе шағылудан кейін) жарығы мен бөлменің ішіндегі қандай да бір таңдалып алынған жазықтықта жасалынатын табиғи жарықтың түгел ашық көктің жарығымен жасалынатын сыртқы көлденең жарықтанудың мәніне қатынасы, %.

Нормаланған шама ретінде салыстырмалы шаманы аламыз- процентпен бейнеленген, табиғи жарықтану коэффициенті ТЖК. ТЖК аспанның жарығымен ғимараттың ішіндегі берілген кеңістікте пайда болатын, табиғи жарықтанудың Еі, толық көк күмбез аспанның жарығымен пайда болатын, тыс көлденең жарықтануға Ет біріңғай қатынасына тең:

$$ТЖК = \frac{E_T \cdot 100}{E_i} \qquad (4.1)$$

мұнда E_T –ғимараттың ішіндегі нүктенің жарықтануы, лк;

E_i –көк күмбез жарығынан көлденең кеңістіктің біріңғай тыс жарықтануы (күн сәулелерін ескермей), лк.

Бүйір жағынан және жоғарыдан жарықтандыру үшін нормаланған ТЖК бөлек. Қарастырып отырған аудитория бүйір жағынан жарықтандырылған. Мұнда жұмыс аймағының шегінде, терезеден ең алыстағы нүктелерде нормаланған минималды ТЖК мәні қамтамасыз етілуі керек. Нормаланған ТЖК мәнін, көрермендік жұмысты жарықтандыру жүйесінің сипаттамасын, ғимараттың орналасу аймағын ескеріп, мына формуламен есептелінеді:

$$e_H = ТЖК \cdot m \cdot c \qquad (4.2)$$

ТЖК – аспан жарығымен бөлме ішінде берілген жазықтықтағы кейбір нүктеде жасалатын табиғи жарықтың, ашық аспанда % толық жарықпен жасалатын сыртқы көлбеу жарықтану мәніне қатынасы.

ТЖК нормаланған мәндері жарықтық климаттың үшінші белдеуі үшін келтірілген, ал басқа белдеулер үшін ТЖК нормаланған мәндері мына формула бойынша анықталады:

$$e_н^{1,2,4,5} = e_н^{3} \cdot m \cdot c \tag{4.3}$$

мұндағы, $e_н^{3}$ – үшінші белдеу үшін ТЖК мәні;

m – жарық климат коэффициенті;

c – күн климаты коэффициенті.

Табиғи жарықтандырудың есебі жарық ойықтарының ауданын анықтаудан қорытындыланады.

Бүйірлік жарықтандыруда ТЖК нормаланған мәндерін қамтамасыз ететін S_0 жарық ойықтарының (терезелер) ауданын мына формула бойынша анықтайды:

$$\frac{100S_0}{S_n} = \frac{e_m \cdot \eta_0 \cdot K_{зд} \cdot K_э}{\tau_ж \cdot r_1} \tag{4.4}$$

Жоғары жарықтандыруда жарық ойықтарының ауданын (қолшамдар) Sф мына формула бойынша:

$$\frac{100S_ф}{S_n} = \frac{e_m \cdot \eta_0 \cdot K_{зд} \cdot K_э}{\tau_ж \cdot r_2 \cdot K_ф} \tag{4.5}$$

мұндағы, S_n – бөлме еденінің ауданы, м^2;

e - ТЖК нормаланған мәні;

$K_з$ – қор коэффициенті;

τ_0 - жарықөткізудің жалпы коэффициенті;

η_0 - терезелердің жарықтық сипаттамасы.

Жұмыс орындарында нормаланған жарықтандыруды жасау үшін бөлменің қажетті бүйірлік жарық ойықтың ауданын есептейміз.

4.1- кесте – Жасанды жарықтану кезіндегі жарықтандыру нормалары және табиғи мен қосарлы жарықтану кезіндегі ТЖК.

Көру жұмыс сипатты	Өзгешелеу Объектінің аз өлшемі	Көру жұмысының разряды	Көру	Фон сипатта-масы	Жарық-тандыру		ТКЖ, %			
					Жасанды		Табиғи		Қос	
					Қосарлы	Ортақ	Жоғ.н/е қос-ы	Жандық	Жоғ.н/е	Жандық
1	2	3	4	6	7	8	9	10	11	12

4.1- кестенің жалғасы

Аса жоғарғы дәлдікті	0,15	I	а	қараңғы	5000	1500	10	3,5	6	2
			б	орташа, қараңғы	4000	1250				
			в	ашық, орташа, қараңғы	2500	750				
			г	ашық, орташа	15000	4000				
Өте жоғарғы дәлдікті	0,3	II	а	қараңғы	4000	1250	7	2,5	4,2	1,5
			б	орташа, қараңғы	3000	750				
			в	ашық, орташа, қараңғы	2000	500				
Жоғарғы дәлдікті	0,3-0,5	IIII	а	қараңғы	2000	500	5	2	3	1,2
			б	орташа, қараңғы	1000	300				
			в	ашық, орташа, қараңғы	750	300				
Орташа дәлдікті	0,5-1,0	IIV	а	қараңғы	750	300	4	1,2	2,4	0,9
			б	орташа, қараңғы	500	200				
			в	ашық, орташа, қараңғы	400	200				
			г	ашық,	3300	1150				

Ұзындықтың тереңдікке қатынасы (яғни терезеден ең қашықталған нүктелері) қатынастары:

$$\frac{\alpha}{в} = \frac{11}{4,2} = 2,61 \qquad (4.6)$$

$$\frac{B}{h_1} = \frac{6}{2,2} = 2,72 \qquad (4.7)$$

мұнда, h_1 – жұмыс орнынан терезенің жоғарғы деңгейіне дейінгі қашықтық:

$$h_1 = 1,2 + 2 - 1 = 2,2 \text{ м}$$

4.2-кесте – Терезелердің жарық сипаттамасының η_0 мәні

$\alpha:B$ қатынасы	$B:h_1$ кездегі							
	1	1,5	2	3	4	5	7,5	10
4≤	6,5	7	7,5	8	9	10	11	12,5
3	7,5	8	8,5	9,6	10	11	12,5	14
2	8,5	9	9,5	10,5	11,5	13	15	17
1,5	9,5	10,5	13	15	17	19	21	23
1	11	15	16	18	21	23	26,5	29
0,5	18	23	31	37	45	54	66	-

Осыдан, $\eta_0 =$ 9.6

Жарықты өткізетін жалпы коэффициентті мына формуламен есептейміз:

$$\tau_{ж} = \tau_1 \cdot \tau_2 \cdot \tau_3 \cdot \tau_4 \qquad (4.8)$$

мұнда τ_1–екі еселенген жақты терезенің әйнегі үшін, өткізетін материалдың түріне байланысты коэффициент $\tau_1 = 0,8$;

τ_1–бөлінген ағаш рамка үшін жаппаның түрін бейнелейтін коэффициент $\tau_2 = 0,6$;

τ_3– темір бетон үшін жаппаның тасушы құрылымын көрсететін коэффициент $\tau_3 = 0,8$;

τ_4–күннен қорғайтын құрылғылардың түріне байланысты, реттелетін, алынып тасталынатын жалюздер үшін коэффициент $\tau_4 = 1$..

$$\tau_{ж} = 0,8 \cdot 0,6 \cdot 0,8 \cdot 1 = 0,384$$

$p_{ср} =$ 0.5 бөлмедегі шағылысуының орта коэффициенті, біржақты бүйірлік жарықтандыруды қабылдаймыз.

r_1 мәнін анықтаймыз:

$$\frac{B}{h_1} = 2,72$$

$$\frac{l}{B} = \frac{4,2}{5} = 0,7 \quad , \; r_1 = 2,2$$

Қасында тұратын ғимарат жүйе тұрған ғимараттан $P = 15$ м қашықтықта орналасқан:

$$H_{зд} = 15 \text{ м}$$

$$\frac{P}{H_{зд}} = \frac{15}{10} = 1,5 \text{ м} \qquad (4.9)$$

4.3-кесте – Қарсы тұрған ғимараттың терезені көлеңкелеуін ескеретін коэффициент Кзд

$P:H_{зд}$	1,5	P– қарастырылып отырған ғимарат пен қарсы ғимараттың ара қашықтығы
$K_{зд}$	1,2	$H_{зд}$ - қарсы ғимараттың карнизінің биіктігі

Осыдан кестеден қарама-қарсы тұрған ғимараттардың терезелерінің көлеңкелеуін ескеретін коэффициент $K_{зд}$ _ны табамыз,ол $K_{зд}=1.2$

$$K_з=1,2$$

$$S_0=\frac{S_n\cdot e_m\cdot\eta_0\cdot K_{зд}\cdot K_з}{100\cdot\tau_{ж}\cdot r_{1a}}$$

$$S_0=\frac{66\cdot 0,675\cdot 9,6\cdot 1,2\cdot 1,2}{100\cdot 0,384\cdot 2,2}=7,78 \text{ м}^2$$

Осылайша табиғи жарықтандырудың жарық ойықтарының ауданы анықталды $S_0=7,78$.

4.2.2 Хабарлағыш санын анықтау

Бір кеңседе датчиктер санын есептеу үшін, олар орнатылған жағының ұзындығын анықтаймыз. Есеп әдістемелік нұсқауларымен жүргізілді [22].

Өрт сөндіргіш ретінде ДИП-3 түтін хабарлағышын қолданамыз. Кеңсенің биіктігі 3 м болғанда, бір хабарлағышпен бақыланатын аудан 10м^2.

ДИП-3 санын мына формула бойынша анықтаймыз:

$$M=Ц\cdot\frac{S}{S_0} \qquad (4.10)$$

мұнда Ц - ең жақын бүтін санға дейін дөңгелектеу;

S - кеңсенің ауданы;

S_o - бір ДИП-3 бақылайтын аудан;

$$M=Ц\left(\frac{3\cdot 2,5}{10}\right)\cdot=0,75=1$$ (аппараттық үшін)

$$M=Ц\left(\frac{18\cdot 12}{10}\right)\cdot=21,6=22$$ (операторлық үшін)

Кеңседе 23 хабарлағышты және хабарлама пульті ретінде "Топаз - 3 М" пультін орнатамыз. Пультке барлық бөлме қосылады. "Топаз-3 М" пульті

хабарлаудың 10 аймағын бақылауға арналған. Сондықтанда біз 3(үш) пультті орнатамыз.

4.2.3 Өрт сөндіргіш

Есеп әдістемелік нұсқау бойынша орындалды [22].

Кернеудегі электр қондырғыларын сөндіру үшін адамдарды су ағысы арқылы электр тогымен зақымданудан қорғаудың арнайы шарасыз суды қолдануға болмайды.

Кеңсеге ОПУ-8 типті ұнтақты өрт сөндіргіш орнатылады. Техникалық сипаттамалар 2-кестеде келтірілген.

4.4-кесте – ОПУ-8 өрт сөндіргішінің сипаттамалары

Параметрлер атауы	Өрт сөндіргіштердің үлгі өлшемдеріне арналған нормалар
Өрт сөндіргіш заттың салмағы, кг	8
Ұнтақ ағысының ұзындығы, м; кем емес.	5
Өрт сөндіргішті іске қосу уақыты, с; көп емес.	5
Ұнтақтың шығу уақыты, с; кем емес.	12
Өрт сөндіру ұнтағының қалдығы,%; артық емес.	10
Пайдалану үшін қол жетімді орта температурасы, С.	-30
	+50
Габариттік өлшемдері:	
Диаметрі, мм	163
Биіктігі, мм	570
Зарядталған өрт сөндіргіштің салмағы, кг.	13,5
В класты сөндіру ауданы, $м^2$; кем емес	3,8
Жұмыс қысымы, МПа	1,2
Корпустың сыйымдылығы, г	8

ОПУ түріндегі ұнтақты унифицирленген өрт сөндіргіштер А класты(қатты заттар), В класты (сұйық заттар), С класты (газ тәріздес заттар) және 1000 В дейінгі электр қондырғыларын өрт сөндіруге арналған.

Барлық өрт сөндіргіштер мерзімді тексеруге және қайта зарядтауға жатады.

Көлемді өрт сөндіру үшін m_d ұнтақты құрамының есептік салмағы,кг мына формула бойынша анықталады:

$$m_d = k \cdot g_n \cdot V \qquad (4.11)$$

мұнда $g_n = 0,4$ - құрамның нормативтік массалық шоғырлануы;

$k = 1,2$ -құрамның ескерілмейтін шығындарын өтеу коэффициенті;

V - кеңсе көлемі.

$$V = A \cdot B \cdot H \tag{4.12}$$

мұнда $A = 3$м - кеңсенің ұзындығы;

$B = 2,5\ м$ - кеңсенің ені;

$H = 4\ м$ – кеңсенің ұзындығы.

Онда:

$$V = 3 \cdot 2,5 \cdot 4 = 30\ м^3$$

Демек:

$$m_d = 1,2 \cdot 0,4 \cdot 30 = 14,4\ кг$$

Егер кеңсенің жабық конструкцияларының алаңы 1% -дан 10% -ға дейін болатын тұрақты ашық тесіктер болса, тесіктердің 1 м2 алаңына 5 кг-ға тең 1 м2 ұнтақ құрамы үшін 5 кг қосымша тұтынылады, яғни (14,4 + 5 = 19,4 кг).

Х баллондарының есептік саны 20 литрлік 12,5 кг ұнтақ құрамының сыйымдылығы есебінен анықталады.

Магистральдық құбырдың ішкі диаметрі d_i, мм, мынадай формула бойынша анықталады:

$$d_i = 12 \cdot \sqrt{2} = 17 \text{ мм} \tag{4.13}$$

Магистральдық құбырдың эквивалентті ұзындығы l_2 м, мынадай формула бойынша анықталады:

$$l_2 = k_1 \cdot l \tag{4.14}$$

мұнда $k_1 = 1,2$ – жергілікті ысыраптарды ескермейтін өтем үшін құбыр ұзындығының ұлғаю коэффициенті;

$l = 3\ м$ – жоба бойынша құбырдың ұзындығы.

Магистральдық құбырдың эквивалентті ұзындығы:

$$l_2 = 1,2 \cdot 3 = 3,6 \text{ м}$$

$A_3, мм^2$ суландырғыштың шығу тесігі қимасының ауданы мынадай формула бойынша анықталады:

$$A_3 = \frac{S}{e1} \tag{4.15}$$

мұндағы S – магистральдық құбыр қимасының ауданы, мм2;

$e1$ – суару саны.

Онда суландырғыштың шығу тесігі қимасының ауданы:

$$A_3 = \frac{3{,}14 \cdot 8{,}52}{1} = 26{,}7 \text{ м}^2$$

Ұнтақ шығыны $Q, кг / с$, құбырдың эквивалентті ұзындығы мен диаметріне байланысты және 1,4 кг / с тең.

Ұнтақ құрамын берудің есептік уақыты $t, мин$, мынадай формула бойынша анықталады:

$$t = \frac{md}{60Q} \text{ мин} \qquad (4.16)$$

$$t = \frac{19{,}4}{60 \cdot 1{,}4} \text{ мин}$$

Ұнтақ құрамының негізгі қорының салмағы $m, кг$, мынадай формула бойынша анықталады:

$$m = 1{,}1 \cdot m_d \cdot \left(1 + \frac{k_2}{k}\right) \qquad (4.17)$$

мұндағы $k_2 = 0,2$ - баллондар мен құбырлардағы ұнтақ құрамының қалдығын ескеретін коэффициент.

Онда:

$$m = 1{,}1 \cdot 19{,}4 \cdot \left(1 + \frac{0{,}2}{1{,}2}\right) = 24{,}9 \text{ кг}$$

Осылайша керекті ұнтақ құрамының негізгі қорының салмағы 24,9 кг.

Бөлім бойынша қорытынды: бұл бөлімінде жұмыс аймағындағы жұмыс жағдайына талдау жасалды. Еңбек жағдайларының деңгейі жұмысшылар үшін қолайлы деп танылды. Жұмыс орынын ұйымдастыру шаралары қарастырылды. Соған байланысты табиғи жарықтандырудың жарық ойықтарының ауданы анықталды (S_0=7,78). Өрт қауіпсіздігі бойынша кеңседегі хабарлағыш және өрт сөндіргіш қондырғыларын жобалау орындалды. Кеңседе қажетті хабарлағыш саны 23, ОПУ-8 типті ұнтақты өрт сөндіргіш орнатылады және көлемді өрт сөндіру үшін ұнтақ құрамының салмағы 24,9 кг екені анықталды.

5 Тәуекелдерді бағалау

5.1 Тәуекелді талдау және бағалау

Дипломдық жұмыстың бұл бөлімінде біз әлеуметтік инженерияның шабуыл жасау тәсілдерінің көмегімен кәсіпорынның шабуыл жасалынатын активтерінің тәуекелдерін бағалаймыз.

Тәуекелдерді басқару құралы болып табылатын тәуекелдерді талдау осалдықтар мен қауіптерді анықтау, ықтимал әсерді бағалау әдісі болып табылады, бұл дәл сол жүйелер мен процестер үшін барабар қорғау шараларын таңдауға мүмкіндік береді. Тәуекелдерді талдау қауіпсіздікті экономикалық тиімді, өзекті, уақтылы және қауіптерге ден қоюға қабілетті етуге мүмкіндік береді. Ол сондай-ақ компанияға тәуекелдер тізімін басымдыққа, қорғау шараларының ақылға қонымды құнын анықтауға және негіздеуге көмектеседі.

Тәуекелді бағалау оның деңгейін (сапалық немесе сандық шамасын) айқындаудан және осы деңгейді ең жоғарғы рұқсат етілген (қолайлы) деңгеймен, сондай-ақ басқа тәуекелдердің деңгейімен салыстырудан тұрады. Басқаша айтқанда, АҚ бұзу тәуекелін бағалау-бұл ақпараттық активтерді олардың өмірлік циклінің барлық сатыларында пайдаланумен байланысты Ақ бұзу тәуекелдерін бағалауды жүргізуге мүмкіндік беретін ақпаратты анықтаудың, жинаудың, пайдаланудың және талдаудың жүйелі және құжатталған процесі.

Маңызды объектілердің тәуекелдерін есептеу үшін екі фактор бойынша тәуекелді бағалау әдістемесі қолданылды [23].

Тәуекел деңгейі екі шаманы біріктіру жолымен анықталады: АҚ саласындағы инциденттің ықтималдығы және оның салдарының мөлшері. Оқиға активтің осалдығын осы активке әсер ету және оның қауіпсіздігін бұзу үшін пайдаланатын қауіпті іске асыру болып табылады.

Ақпараттық активтің қауіпсіздігі деп ақпараттың құпиялылығы (рұқсатсыз танысудан қорғау), тұтастығы (ақпараттың өзектілігі мен қарама-қайшы еместігі, оның бұзылудан және рұқсатсыз өзгертуден қорғалуы) және қолжетімділік (қолайлы уақытта талап етілетін ақпараттық қызметті алу мүмкіндігі) сияқты қасиеттері түсініледі.

Қауіпті іске асыру ықтималдығы сараптамалық бағалау, болжау жолымен, сондай-ақ статистикалық деректер негізінде айқындалады. Белгілі бір уақыт кезеңінде қауіп-қатерді іске асыру әрекеттерінің күтілетін санын анықтайтын оң сан болып табылады.

Әрбір жобалық тәуекелді сипаттайтын келесі маңызды компонент шығын мөлшері болып табылады.

Ақпаратты ашуға, рұқсатсыз модификациялауға, уақытша қолжетімділікке немесе бұзуға байланысты қауіпсіздік инциденттері нәтижесінде ұйымға келтірілген залалдың мөлшері ақпараттық активтердің құндылығымен

айқындалады. Мұндай инциденттердің салдарлары жіберілген пайдада, бәсекелік артықшылықтардың жоғалуында, ұйым имиджінің нашарлауында, үшінші тараптың мүдделеріне зиян келтіруде, айыппұлдарда, тікелей қаржы шығындарында немесе қызметті іріткісіздендіруде көрініс табуы мүмкін. Бұл ретте әрбір актив үшін оқиғаларды дамытудың ең нашар сценарийін қарау керек [24].

5.1-кесте – Қауіптің туындау ықтималдығы шкаласы

Қауіптің туындау ықтималдығы шкаласы	
Ықтималдылық деңгейі	Қауіптің туындау ықтималдығы
1 – Өте төмен	Шамамен 2-3 рет 10 жылда
2 - Төмен	Шамамен 5 жылда бірнеше рет және сирек
3 - Орташа	Шамамен жылына бірнеше рет
4 - Жоғары	Айына шамамен 1 рет
5 – Өте жоғары	Шамамен айына бірнеше рет

Келесі кестеде деңгейлер бойынша тәуекел салдарының шамасы көрсетілген.

5.2-кесте – Залал шамасының шкаласы

Залал шамасының шкаласы	
Мәні	Сипаттамасы
1 – Өте төмен	құны 50 000 теңгеге дейін
2 - Төмен	құны 200 000 теңгеге дейін
3 - Орташа	құны 500 000 теңгеге дейін
4 - Жоғары	бағасы 1 000 000 теңгеге дейін
5 – Өте жоғары	құны 1 000 000 теңгеден жоғары

Дипломдық жұмысты әзірлеу кезінде қолданылатын маңызды объектілерді анықтау арқылы қорғауды талап ететін активтер тізімі жасалды:

- жұмыс станциясы;
- Web-сайт;
- сервер;
- Outlook поштасы;
- деректер базасы.

5.3 кесте – Тәуекелдерді бағалаудың қорытынды кестесі

№	Қауіптер	Осалдықтар	Жоғарғы мәні	Қорғаныс шаралары	Қалдық мәні
1 Жұмыс станциясы					
1.1	Құжаттарды, тасымалдаушылардың ұрлануы	Рұқсатсыз көшіру	4	Құпия ақпараттың ақпараттық жүйеден ағып кетуінің алдын алу	3
1.2	Бағдарламалық бұзылуы	DDOS шабуылдар немесе техниканы істен шығаруға бағытталған басқа да шабуылдар	2	Басып кіруді анықтау жүйесі, жүйені резервтік қалпына ке	1
1.3	Деректерді өзгерту	Ақпараттық жүйемен жұмыс істеу кезінде белгіленген ережелерді білмеу немесе сақтамау және деректерді өзгерту	4	Рұқсат етілмеген қолжетімділікті жүзеге асыру мүмкіндігін болдырмау	3
2 Деректер қоры					
2.1	Деректерді өзгерту	Деректерді рұқсатсыз түрлендіру	6	Деректер зақымдануының алдын алу	3
2.2	Құпия ақпаратты шифрлеу және оқу	Күрделі ақпаратты шифрленбеген түрде сақтау	6	Серверлерде сақталатын деректерді қорғауға арналған криптографиялық шешімдер кешені	3

5.3-кестенің жалғасы

2.3	SQL-инъекция	SQL сұраулары үшін сүзгілеу ережелерінің дұрыс еместігі	3	Веб-қолданбаның желіаралық экраны	0
3 Web-сайт					
3.1	Веб-Сервердің/ қосымшалардың іздері браузерлер, клиенттер, серверлер және пайдаланылатын операциялық жүйелер туралы ақпарат алуға мүмкіндік береді.	Ақпарат ағуы сервер маңызды ақпаратты, мысалы, жүйені бұзу үшін пайдаланылатын қателер туралы хабарламаларды жариялайды	12	Кіруді басқару жүйелері, қоршау және физикалық оқшаулау, конфигурация элементтерінің резервтік көшірмелері	8
3.2	Құпия сөзді, пайдаланушы атын және қате шифрлау кілтін автоматты түрде таңдау	Маңызды ақпаратқа шынайылығын тексермей қол жеткізу мүмкіндігі	9	Қол жеткізуді басқару, парольмен қорғауды ұйымдастыру	6
3.3	Сеансты растау (сеанстың идентификаторын белгіленген мәнге қою мүмкіндігі)	Сеанс идентификаторының болжамды мәні зиянкестерге басқа пайдаланушының сеанстарын ұстап тұруға мүмкіндік береді	6	Қол жеткізуді басқару жүйелері, қоршау және физикалық оқшаулау, конфигурация элементтерінің резервтік көшірмелері	4

5.3-кестенің жалғасы

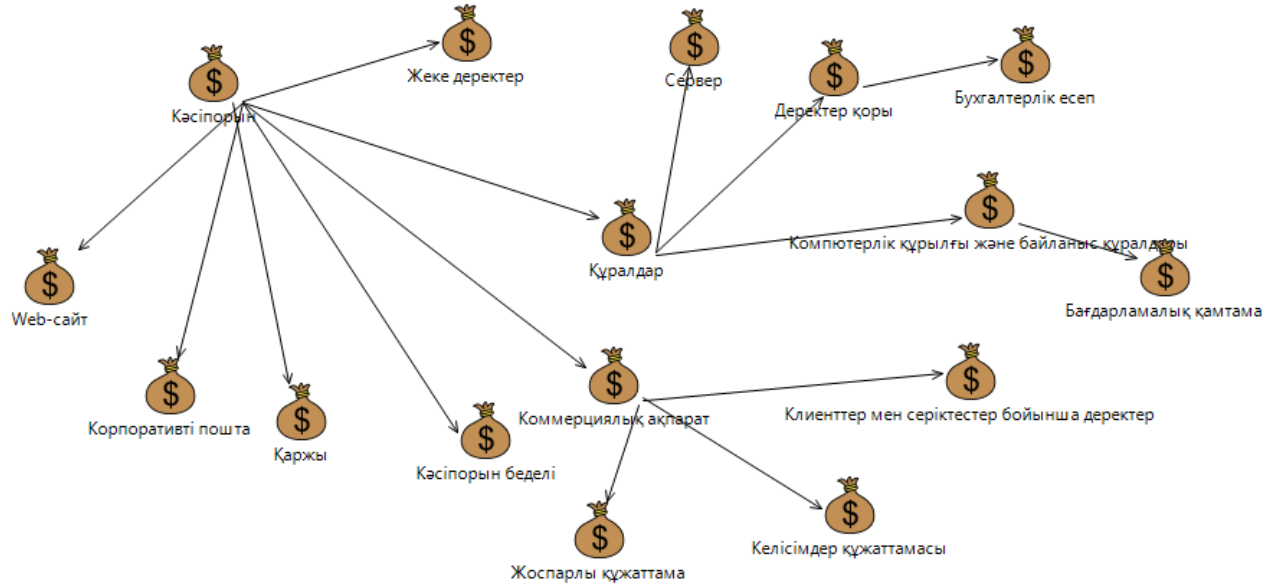
4 Outlook поштасы					
4.1	Қызмет көрсетуден бас тарту	Жұмыс жад буферінде толып кетуі	3	Басып кіруді анықтау жүйесі, жүйені резервтік қалпына келтіру	2
4.2	Ақпараттың құпиялылығын бұзу	Арнайы HTML тегтері бар жазу арқылы веб-бет мазмұнын ауыстыру	4	Трафикті сүзгілеу	3
4.3	Деректерді ұстау	Бастапқы және ресурстық IP адрестерін алмастыру мүмкіндігі	4	Деректер мен пакеттерді жинайтын және талдайтын желідегі машинаны анықтайды	3
5 Сервер					
5.1	Серверді рұқсатсыз басқару	Қол жеткізу құқықтарын дұрыс бөлмеу	8	Рұқсат етілмеген қолжетімділікті жүзеге асыру мүмкіндігін болдырмайды	4
5.2	Жабдықтың істен шығуы	Үздіксіз жұмыс істеу кезіндегі кемшіліктер	12	Басып кіруді анықтау жүйесі, жүйені резервтік қалпына келтіру	8
5.3	Серверлік кеңейтулерді енгізу	Пайдаланушы ұсынған деректерді сервер түсіндіретін файлда сақтамас бұрын тексерудің болмауы.	8	Рұқсатсыз кіруді болдырмайды	4

5.2 CORAS құралы арқылы тәуекелдерді талдау

Coras құралы бағдарламалық жасақтаманы әзірлеу саласында объектілі модельдеу үшін UML – графикалық сипаттау тілін қолданады [24].

Тәуекелдерді талдаудың көрнекілігі үшін Coras бағдарламалық құралын пайдаландық. Жоғарыда сипатталған активтер диаграммасынан кейін және олардың арасындағы байланысы 5.1-суретте көрсетілген.

Бағдарламада қорғауға жататын құндылықты (ақпаратты) білдіретін Asset элементі пайдаланамыз.

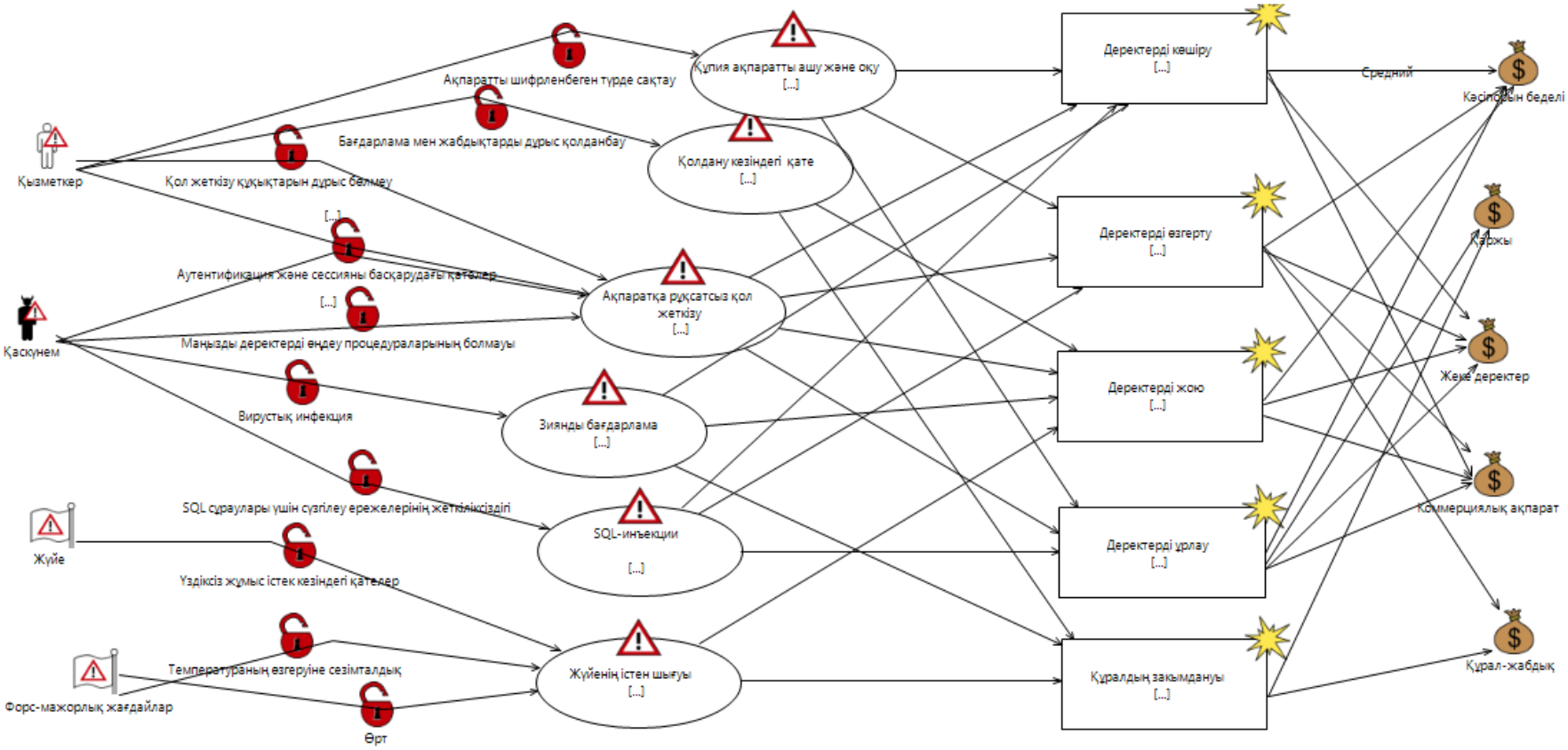


5.1-сурет – Активтер диаграммасы

5.4-кестені пайдалана отырып, тәуекелдерді үлгілейміз, яғни әуекелдер диаграммасын генерациялаймыз, бұдан әрі әрбір актив үшін әрбір тәуекел бойынша осы тәуекел жүзеге асырылған жағдайда салдарларды анықтаймыз. Алынған диаграмма 5.4-суретте көрсетілген.

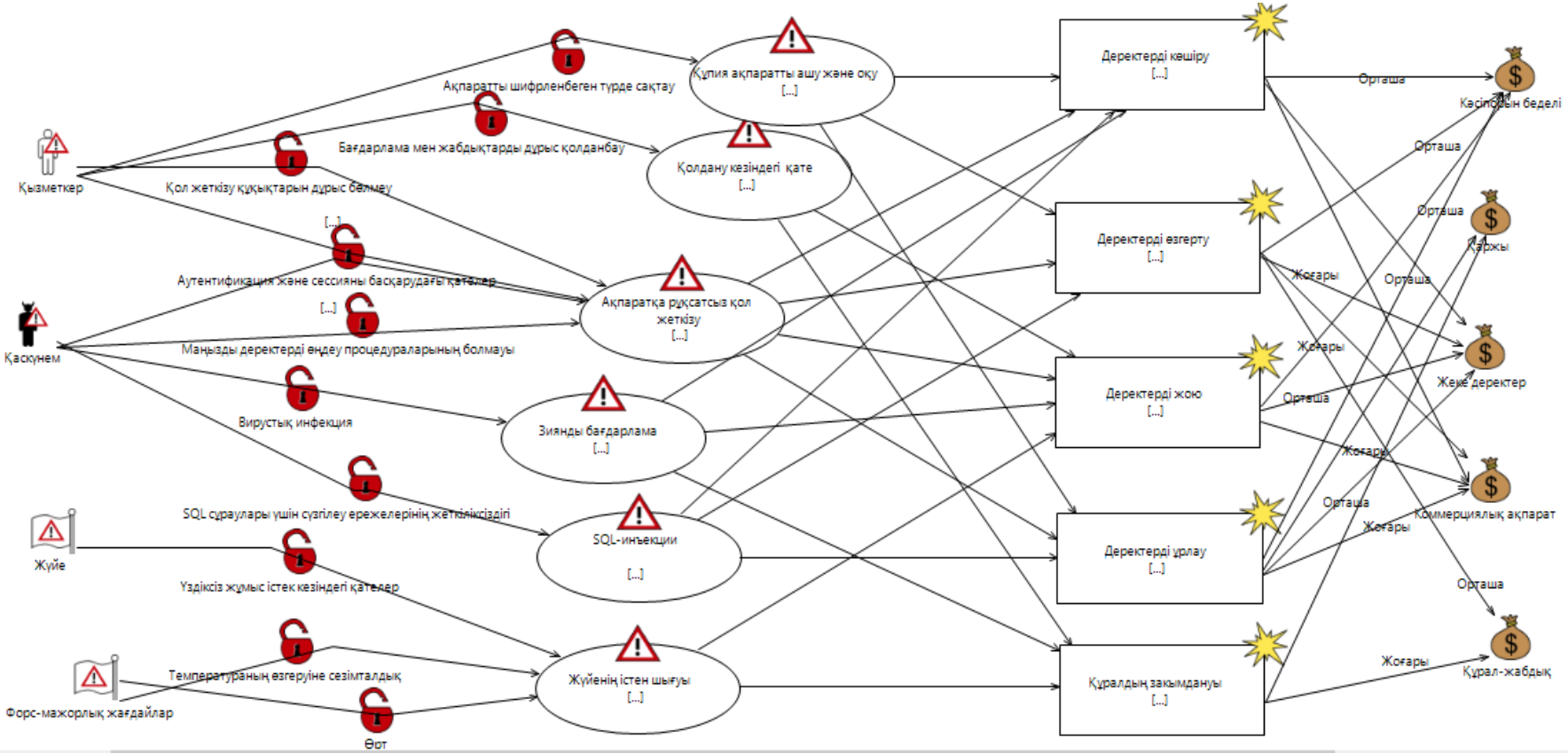
Бағдарламада келесі элементтер пайдаланылады:

- Threat Human Accident – адам факторымен байланысты қасақана емес қауіп-қатерлерді белгілеу үшін
- Threat Human Deliberate – адам факторына байланысты қасақана қауіп-қатерлерді белгілеу үшін
- Threat Non Human адам факторымен байланысты емес қауіптерді белгілеу үшін;
- Threat Scenario – қатерлерді сипаттау үшін;
- Vulneravility – осалдықтарды сипаттау үшін;
- Unwanted Incident – жағымсыз оқиғаларды белгілеу үшін.



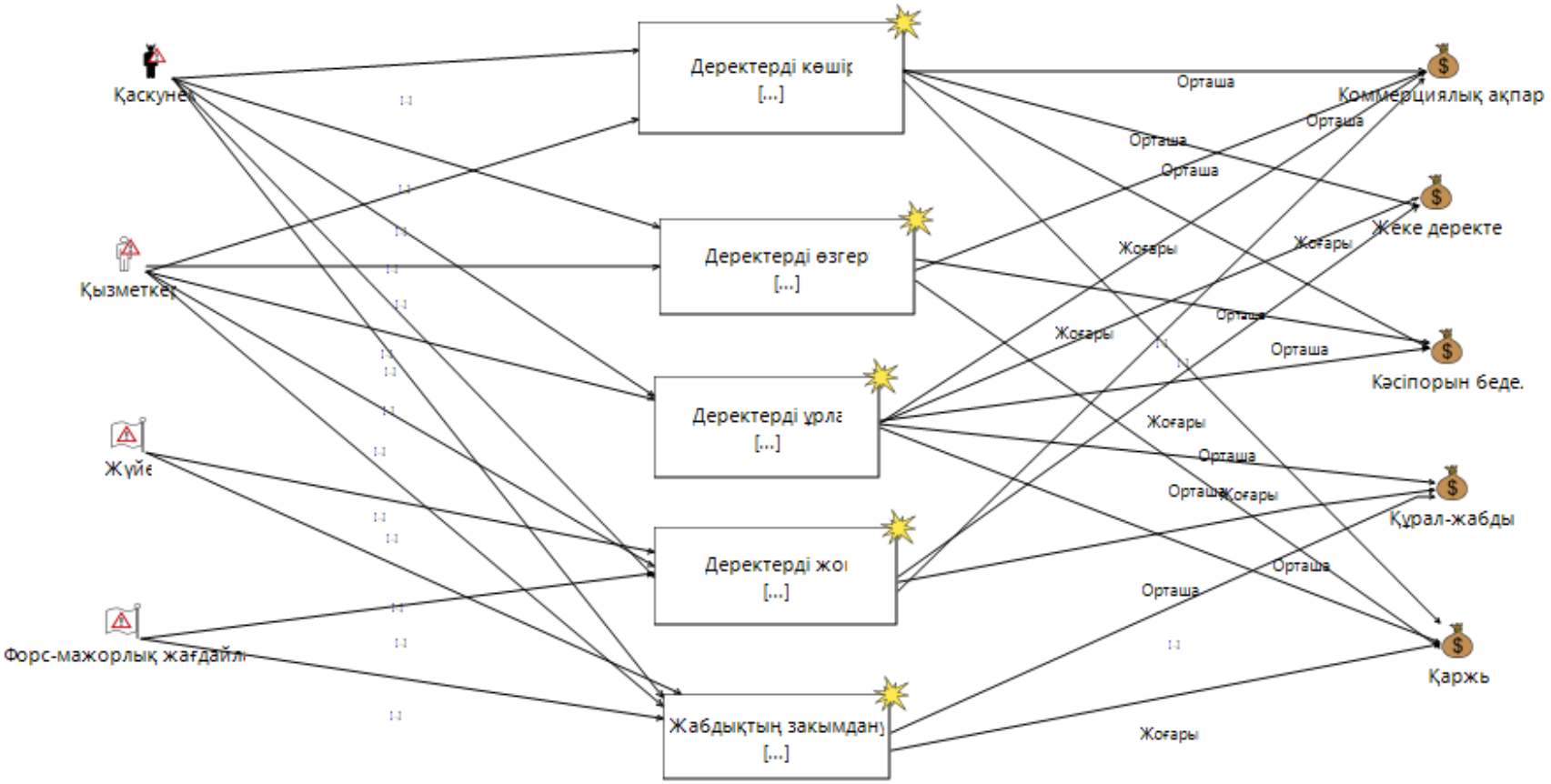
5.2-сурет – Қауіптер моделі

Бұдан әрі пайда болған тәуекелдерді іске асыру жиілігін анықтаймыз (белгілі бір уақыт кезеңінде қауіп-қатерді іске асырудың күтілетін саны).



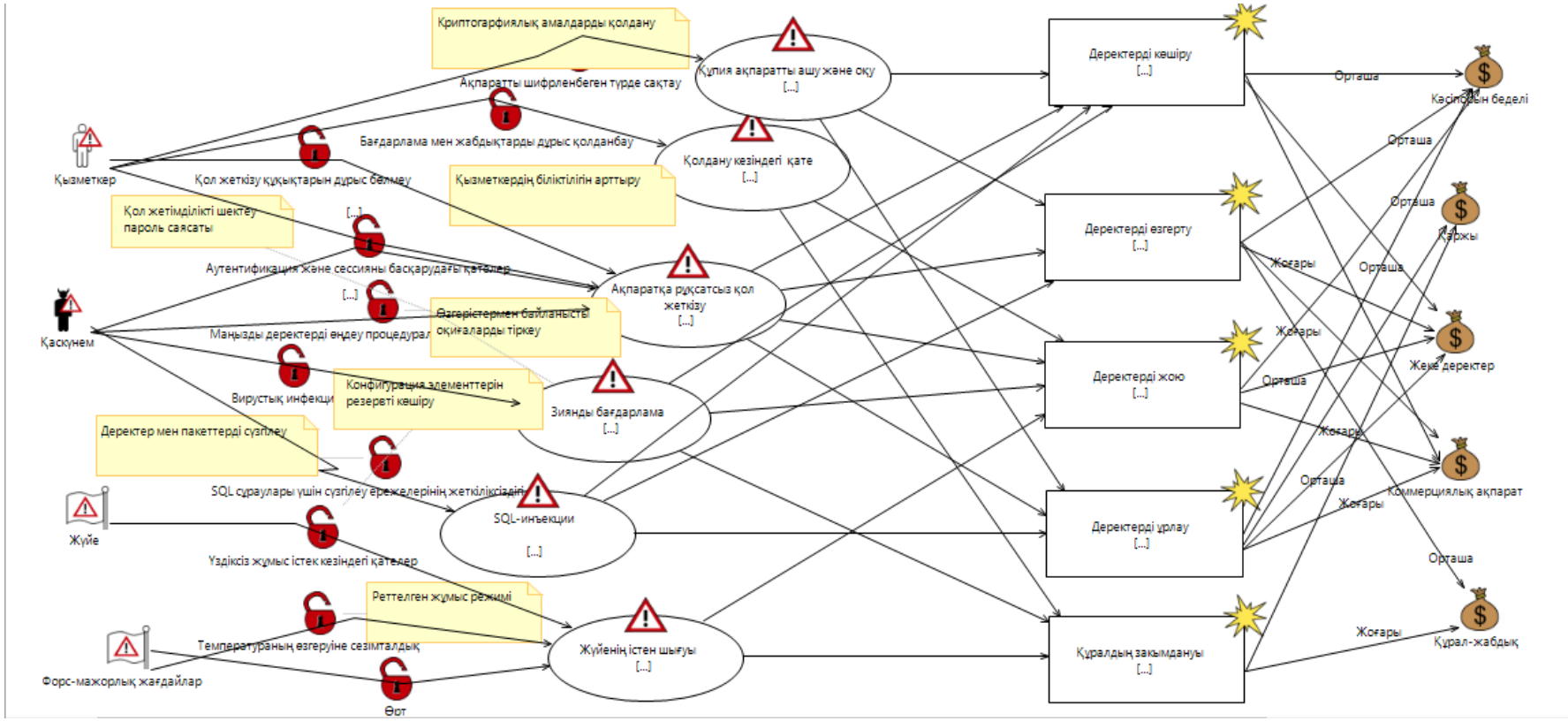
5.3-сурет – Ықтимал сипаттамалары бар қауіптер моделі

Ақпараттық қауіпсіздік инциденті бірнеше активтерге немесе активтің бір бөлігіне әсер етуі мүмкін. Әсер ету оқиғаның сәттілік деңгейімен байланысты. Әсер қаржылық немесе нарықтық салдарды қамтитын жедел әсердің немесе болашақ (іскерлік) әсердің болуы деп саналады. Әрі қарай әрбір актив үшін тәуекелге ұшырау дәрежесін бағалаймыз (5.4-сурет)



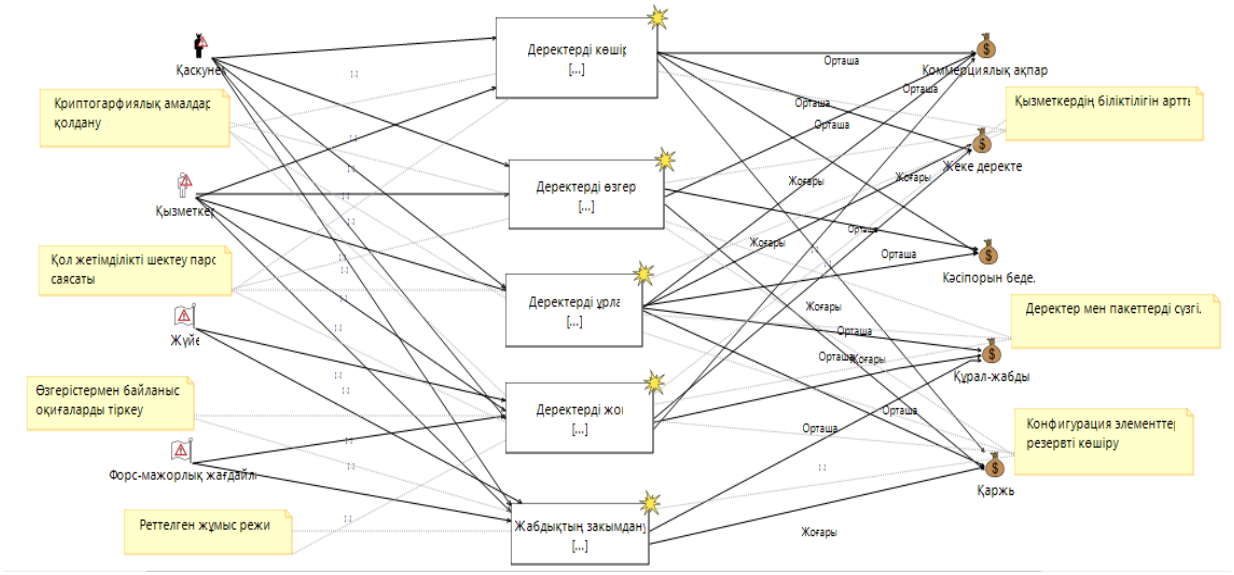
5.4-сурет – Қауіпті жүзеге асыру салдарларының сипаттамасы бар тәуекелдер диаграммасы

Іс-шараларды таңдау және нақтылау ақпараттық қауіпсіздікке төнетін қатерді талдау нәтижелеріне негізделуі керек. Біз олардың өмірлік циклі процестерінде бағдарламалық осалдықтардың пайда болуын және жойылуын болдырмау мақсатында қауіп-қатерді жүзеге асыратын қорғау шараларының тізбесін анықтаймыз (5.5-сурет).



5.5-сурет – Қорғаныс шараларын қосқаннан кейінгі қауіптер диаграммасы

Қорғау шараларын қосқаннан кейін қабылданбайтын тәуекелдер қалуы мүмкін. Мұндай жағдайларда шешім қабылдайтын тұлғаларға қалыпты қабылдау критерийлерін қабылдамайтын тәуекелдерді сақтауға тура келуі мүмкін. Егер бұл қажет болса, шешім қабылдайтын тұлға тәуекелдерге нақты түсінік беріп, шешім үшін ақтауды енгізуге тиіс тәуекелдің қалыпты қабылдау критерийлерін жою (5.6-сурет).



5.6-сурет – Қолайсыз тәуекелдер диаграммасы

Бөлім бойынша қорытынды: дипломдық жұмыстың осы бөлімінде әлеуметтік инженерия шабуылының әдістері арқылы шабуылдаушы компанияның активтерінің тәуекелдері анықталды.

Барлық анықталған ресурстар бойынша тәуекелдерге талдау жүргізілді және ақпараттық жүйені қорғау шаралары анықталды. Тәуекелдерді бағалау үшін екі фактор бойынша есептеу әдісі қолданылды.

Қауіп-қатерлерді бағалау процесіне арналған негізгі жұмыстар қаралды. Таңдалған активтердің негізгі қатерлері мен осалдықтары қаралды.

Тәуекелдер деңгейін бағалаудың бастапқы және қайталама есебі жасалды, сондай-ақ тәуекелді өңдеу бойынша шаралар қабылданды.

Екінші бөлікте CORAS көмегімен ақпараттық тәуекелдерге талдау жүргізілді және активтерді сәйкестендіруден бастап, қауіп-қатер мен осалдықтар моделінен бастап, қарсы өлшемдерді енгізумен аяқталатын UML диаграммалары салынды.

Қорытынды

Бұл ғылыми жұмыста әлеуметтік инженерия жан-жақты зерттелді. Әлеуметтік инженерияны зерттеу - қазіргі кезде ақпараттық ауіпсіздік мәселелерін зерттеуде өте өзекті болып табылады. Әлеуметтік инженерия атты мәселені шешу немесе оны алдын алу үшін, әлеуметтік инженерия не екені зерттелу керек, ол үшін Әлеуметтік инженерияның амалдырын зерттеп, обьект және субьектілерін анықтап алу қажет. Амалдардың әр қайсысына жеке- жеке сараптамалық зерттеулер жасалды, нәтижесінде қаскүнемнің қалай алаяқтық жасайтыны және зардап шегушінің қандай жолмен қаскүнем құрған қақпанға түсетіні тәжірибе жүзінде көрсетілді. Зардап шегуші тек қана жеке адам емес, белгілі бір орта немесе үлкен компаниялар болуы мүмкін. Әлеуметтік инженерия мәселесінен қорғану немесе алдын алу мақсатында, эксперттердің жазған кеңестері назарда ұсталып, тұжырымдамалар жасалды. Әлеуметтік инженерияның кейбір амалдарынан қорғану мақсатында, бірнеше алдын алу әдістері ойлап табылды және ол тәжірибе жүзінде іске асырылып дұрыс екені дәлелденді.

Әдебиеттер тізімі

1. Варлатая С. К., Шаханова М. В. Аппаратно-программные средства и методы защиты информации. – Владивосток: Изд-во ДВГТУ, 2007. – 318 с.
2. Social Engineering //Электронды мәлімет көзі. Элек.журн. Кевин Бивер 2017. Мәліметке қол жеткізу: https://searchsecurity.techtarget.com
3. Грызунов В.В., Бондаренко И.Ю. Социальный инженер с точки зрения теории управления Electronic ISBN: 978-1-5386-5612-9. Print on Demand ISBN: 978-1-5386-5613-6. - 2018. - pp.592-597
4. Кузнецов М. В. Симдянов И. В. Социальная инженерия и социальные хакеры. – М.: СПб.: БХВ-Петербург, 2007. – 45 с.
5. Сиротский А.А. Технологии социальной инженерии как потенциальная угроза в социальной сфере. В сборнике: Информационная безопасность бизнеса и общества Сборник избранных статей научно-педагогического состава кафедры информационных систем, сетей и безопасности. Российский государственный социальный университет. – М.: Изд-воВМиК МГУ, 2016. – 67 с.
6. Шаньгин, В.Ф. Информационная безопасность и защита информации. — М.: ДМК, 2017. – 702 с.
7. Митник К., Саймон В. Искусство обмана. — М.: Изд-во МАКС Пресс, 2006 г. – 50 с.
8. Фомина Н.А. Использование методов социальной инженерии при мошенничестве в социальных сетях. Под редакцией Г.Н. Чусавитиной, Е.В. Черновой, О.Л. Колобовой. – М.: Изд-во МАКС, 2015. – С. 443-453.
9. Социальная инженерия //Электронды мәлімет көзі. Элек.журн. EFSOL жүйе интеграциясы 2017. Мәліметке қол жеткізу: https://narfu.ru /agtu/www. agtu.ru
10. Шудрова К. Социальная инженерия в информационной безопасти. – М.: Изд-во ГЛТ, 2012. – №10. – с. 13-17.
11. More than one in 10 employees fall for social engineering attacks //Электронды мәлімет көзі. Элек.журн. Warrick Ashford 2018. Мәліметке қол жеткізу: https://www.computerweekly.com
12. Запечников С.В., Милославская Н. Г. Информационная безопасность открытых систем. Угрозы, уязвимости, атаки и подходы к защите. – М.: ГЛТ, 2017. – 536 с.
13. Жандаулетова, Ф. Р. Охрана труда: учебник для вузов / Ф.Р. Жандаулетова, Т.Е. Хакимжанов, Т.С. Санатова; МОН РК, НАО АУЭС. – Алматы, АУЭС, 2019. - 399 с.
14. ҚР Құрылыс және тұрғын үй-коммуналдық шаруашылық істері агенттігі: ҚР ҚНжЕ 2.02-05-2009/ Ғимараттар мен имараттардың өрт қауіпсіздігі. Сәулет, қала құрылысы және құрылыс саласындағы мемлекеттік нормативтер: - Астана, 2010. – 107 б.

15. ГОСТ 50923-96 «Дисплеи. Рабочее место оператора. Общие эргономические требования и требования к производственной среде. Методы измерения», Стандартинформ, 2008 - 11 б.

16. ҚР ҚНжЕ 2.04-05-2002 – «Жасанды және табиғи жарықтандыру» - Сәулет, қала құрылысы және құрылыс саласындағы мемлекеттік нормативтер, Астана, 2002. – 110 б.

17. Информационно-издательский центр Минздрава России: СанПиН 2.2.4.548-96/ Гигиенические требования к микроклимату производственных помещений. Санитарные правила и нормы: - М, 2001. – 20 с.

18. ҚР ҚНжЕ 2.04-01-2001. «Құрылыстық климатология» - Сәулет, қала құрылысы және құрылыс саласындағы мемлекеттік нормативтер, Астана, 2002.

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

20. Құрылыс комитеті, Индустрия және сауда министрлігі: ҚР ҚН 2.02-11-2002/ Ғимараттарды, бөлмелерді және имараттарды автоматты өрттік сигналдаудың жүйелерімен, автоматты өрт сөндіру және өрт туралы адамдарға хабарлау қондырғыларымен жабдықтау нормалары: - Астана, 2002. - 118 б.

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

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

23. ISO/IEC 27005 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. М: Стандартинформ, 2008. – 40 с.

24. Баранова, Е.К. Методики и программное обеспечение для оценки рисков в сфере информационной безопасности / Е.К. Баранова // Управление риском. – 2009. – № 1 (49). – С. 15-26.