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. Қорғау.

Мамандығы: 5В100200 – «Ақпараттық қауіпсіздік жүйелері»
Орындаған: Бекенов Әсет Еркінұлы 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: Бекенов Әсет Еркінұлы
(аты-жөні)

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

2019 ж. «11» қараша №56 университет бұйрығымен бекітілді.
Л3

Аяқталған жұмысты тапсыру мерзімі: «____»_____20___ ж.

Жобаға алғашқы деректер (талап етілетін зерттеу (жоба) нәтижелерінің параметрлері және зерттеу нысанының алғашқы деректері): _____

Ұсынылған дипломдық жұмыста – Әлеуметтік инженерия тарихы, Әлеуметтік инженерия әдістері. Әлеуметтік инженериядан қорғанудың осы күнге дейінгі әдіс-құралдары.

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

1. Әлеуметтік инженерияның өзектілігі.
2. Әлеуметтік инженерия тарихы.
3. Әлеуметтік инженерия қарулары.
4. Әлеуметтік инженериядан қорғану және оның алдын алу жолдарындағы амалдар
5. Жұмыс жағдайында табиғи жарықтандыруды, өрт қауіпсіздігін және желдету жүйесін есептеу.
6. Ақпараттық қауіпсіздік тәуекелдерін екі параметр бойынша бағалау.

Графикалық материалдардың (міндетті түрде дайындалатын сызбаларды көрсету) тізімі:

2.1 сурет – Әлеуметтік инженерияның қолданудың негізгі облыстары
3.1 сурет – Қызметкерлерге арналған тест
3.3 сурет – Тест сұрақтары.
3.4 сурет – Әлеуметтік инженерияға қарсы бағдарлама
3.7 сурет – Бағдарламаның күдікті сайтты бұғаттауы.
3.8 сурет – Құнды ақпаратты алдын ала қорғау.
3.11 сурет – Шабуылдаушының ақпаратқа қол жеткізе алмауы
4.1- сурет – Бөлменің схемасы
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.
4. Кевин Митник, Искусство обмана / Компания АйТи; 2004.

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 инженерияны өзектілігі	18.02.20 – 10.03.20	орындалды
1.2 Әлеуметтік инженерияның түсінігі, тарихы	18.02.20 – 10.02.20	орындалды
1.3 Әлеуметтік инженерияның қолдану салалары, мақсаттары	18.02.20 – 10.02.20	орындалды
2 Әлеуметтік инженерия қарулары	12.03.20 – 24.03.20	орындалды
3 Әлеуметтік инженериядан қорғану және оған қарсы қолданылатын амалдар	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 _____ (Бекенов Ә. Е.)
(қолы) (аты

АҢДАТПА

Ұсынылған дипломдық жұмыста – «әлеуметтік инженерия ақпараттық қауіпсіздік аспектісінде» пәні бойынша зертханалық жұмыстар әдістемесі әзірленіп және қорғану амалдары ұйымдастырылды. 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, және қорғану мақсатында тесттер жасалынды, антивирустық бағдарламалар қолданылды. Осы ретте Trend Micro Internet Security, «AnsTester» бағдарламалары пайдаланылды. Әлеуметтік желіде алаяқтардан қалай сақтану керектігі көрсетілді. Әлеументтік инженериялық тренинг әзірленді.

АННОТАЦИЯ

В этой дипломной работе мы разработали методика лабораторных работ по предмету «Социальная инженерия в аспекте информационной безопасности» и организовали меры защиты. Несколько методов атаки в социальной инженерии были применены на практике, и на основе полученных данных были предложены способы защиты или предотвращения. В частности, были проведены тесты и использовались антивирусные программы, чтобы завоевать доверие и доступ к информации пользователя социальной сети, фишингового сайта и защиты. Были использованы Trend Micro Internet Security и AnsTester. Было показано, как избежать мошенников в социальных сетях. Был проведен социальный инженерный тренинг.

ANOTATION

This is a thesis “Development of the laboratory work methology on the discipline “Social Engineering in the aspect of information security and the organization of protection. Several attack methods in social engineering were put into practice, and based on the data obtained, methods of protection or prevention were proposed. In particular, tests were conducted and anti-virus programs were used to gain trust and access to information of a user of a social network, phishing site and protection. Trend Micro Internet Security and AnsTester were used. It was shown how to avoid scams in social networks. A social engineering training was conducted.

Мазмұны

Кіріспе

Бұл дипломдық жұмыс ақпараттың қауіпсіздігі және әлеуметтік инженерия жайында көптеген ақпарат береді.

Ең дамыған қорғаныс жүйесі де кейде пайдасыз болып қалуы мүмкін, егер онымен психологиялық тұрғыдан тұрақсыз немесе ақымақ адам басқарса. Хакерлік жаргонда адамға шабуыл әлеуметтік инженерия деп аталады және оның канондық формасында ол әдетте басқа тұлға арқылы таныстырып құпия ақпаратты (парольдерді) алу үшін телефон соғу.

Қазір әлеуметтік инженерияға қызығушылық өте жоғары. Мұны мынадай белгілер арқылы байқауға болады, мысалы, бірнеше жыл бұрын Google іздеу жүйесінде «әлеуметтік инженерия» туралы тек 2-3 сілтемелер ғана болатын ал қазір олардың саны жүздеген. Garther коорпорациясының АҚ бөлімінің бастығы Рич Могулл Әлеуметтік инженерия желіні әдеттегі бұзғаннан да қауіпті, дейді. Ең қауіпті бұзулар электрондық бұзу емес, әлеуметтік инженерияның арқасында болып жатыр. Алдағы 10 жыл тіптен бұл қауіпті өршітеді, - дейді. Оны Sophos антивирустың компаниясы бөлімшесінің басқарушы директоры Роб Форсайт та қолдайды.

Бүгінде ақпараттық қауіпсіздіктің адами факторы 20 жыл бұрын, Интернет коммерциялық емес және оның пайдаланушылары тек мамандар болған кезде әлдеқайда маңызды рөл атқарады. Ақпараттық қауіпсіздік мәселесін аппараттық және бағдарламалық құралдардың көмегімен шешуге болады деп ойлайтын көптеген компаниялар қатты жаңылысады.

Біз сенуге үйренген қауіпсіздік технологиялары – желіаралық экрандар, сәйкестендіру құрылғылары, шифрлау құралдары, Желілік шабуылдарды анықтау жүйелері және басқалары-әлеуметтік инженерия әдістерін пайдаланатын хакерлерге қарсы тұруда тиімділігі аз. Қызметкерлермен күшті жұмыс істеу, қызметкерлерді қауіпсіздік саясатын қолдануға және әлеуметтік инженерлерге қарсы тұру техниктеріне оқыту қажет – сонда ғана сіздің қауіпсіздігіңіз кешенді болады.

Себебі, техникалық қорғау құралдары күннен күнге дамуда, ал адамның әлсіз жақтары, ойламдары, стереотиптері өзгермейді. Ең керемет деген қорғау жабдығын қолданғанның өзінде де абай болуымыз керек.

1 Әлеуметтік инженерия

1.1 Әлеуметтік инженерия өзектілігі

Бүгінгі таңда ақпараттық қауіпсіздіктегі адам факторы бұрынғыға қарағанда әлдеқайда маңызды рөл атқарады. Біз сеніп жүрген қауіпсіздік технологиялары, яғни - брандмауэр, сәйкестендіру құрылғылары, шифрлау құралдары, желілік шабуылды анықтау жүйелері әлеуметтік инженерия әдістерін қолданатын хакерлерге қарсы тұру үшін әлі де жеткіліксіз болып табылады.

Кибер алаяқтар азаматтардың қаражатын тартып алу үшін әлеуметтік инженерия деп аталатын (әлеуметтік және психологиялық дағдыларды қолдана отырып, адамның мінез-құлқын айла-шарғы жасау) тәсілді жиі қолданады. Кез-келген әлеуметтік инженердің міндеті - адамға қалыпты өмірде жасамайтын әрекеттерді жасауға итермелеу. Қазіргі таңда әлеуметтік инженерия арқылы жасаған шабуылдардан зардап шегушілер шамамен 25 000- 100 000 доллар арасында қаражат жоғалтады, бұған дәлел Zecurion сарапшыларының пікірінше, 2016 жылы әлеуметтік инженерлерді қолданатын алаяқтар ресейлік банк карталарынан шамамен 650 миллион рубль ұрлаған, ал 2017 жылы залал шамамен 750 миллион рубльге дейін ұлғаюы мүмкін.

Альфа Банктің электрондық бизнесті бақылау бөлімінің бастығы Владимир Бакулиннің айтуы бойынша: Бүгігі таңда әлеуметтік инженерия өте тез дамып келе жатыр, бұл тәсілді қолданатын кибералаяқтарда және осы тәсілден зардап шеккен қарапайып адамдар саныда күн санап артуда. Егер бұрындары әлеуметтік инжинирингтің танымал түрі тривиальды SMS-хабарламалар жіберетін болса, одан зардап шегетіндер көбінесе қарт адамдар болатын. Ал қазір құрбан болғандардың портреттері мен алаяқтықтың әртүрлі болуы байқалып отыр жәнеде қазір алаяқтар күрделі тәсілдерді қоладанады.

1.2 Әлеуметтік инженерия түсінігі, тарихы.

Ақпараттық қауіпсіздікті қамтамасыз ету әдістерінің дамуымен адамдар қазіргі қауіпсіздік жүйесіне сенім арта бастады, жеке ақпаратты қорғау процесіне қатысты барлық мәселелер бағдарламалық қамтамасыздандыруға, сонымен қатар дайын IT-шешімдерге көшті. Осылайша, қоғам шабуылдаушыларға ұрлау немесе басқа адамдардың ақпаратына рұқсатсыз кірудің жаңа тәсілдерін іздеуді қажет етті. Осылайша, әлеуметтік инженерия басталды.

Әлеуметтік инженерия - әлеуметтану мен психологияны пайдалана отырып нақты қажетті нәтижеге барынша тиімді әкелетін кеңістікті,жағдай мен шарттарды құру тәсәлдерінің, әдістері мен технологияларының жиынтығы.

Көбінесе «әлеуметтік инженерияның атасы» әйгілі хакер К. Митник ретінде белгілі. Митник алғашқылардың бірі болып «бағдарламалық

жасақтаманы» емес, компьютерде жұмыс істейтін адамды айласына түсіріп, компьютерде отыраған адамды манипуляциялау өнерін қолданды. Сол кезден бастап адамды манипуляциялау арқылы ақпаратқа қол жеткізуді әлеуметтік инженерия деп атала бастады.

Хакерлардың, нақтырақ айтсам фрикерлердің алқғашқы қызғушылықтарының бірі болып операторларға телефон соғып олардың жұмыстары туралы біліп, кез-келген сұрақтар қойып мазақ қылу болатын. Уақыт өте келе фрикерлер осы әдісті ақпаратқа заңсыз түрде қол жеткізу мақсатында қоладана бастады.

Адамдардан қандай да бір ақпарат алу үшін немесе жай ғана бірдеңе жасау үшін телефон арқылы сөйлесу өнер болып саналды. Бұл саланың мамандары өз шеберліктерін өте мақтан тұтты. Ең білікті әлеуметтік инженерлер әрқашан өздерінің инстинкттеріне сүйене отырып, тапқырлық танытты. Жетекші сұрақтар бойынша, дауыстың интонациясы бойынша, олар адамның қиындықтары мен қорқыныштарын анықтап, лезде бағдарлай отырып, олармен ойнай алады. Егер желінің екінші жағында жақында жұмысқа келген бір жас қыз болса - фрайзер бастықпен мүмкін болатын қиындықтар туралы айтады, егер ол өз-өзіне тіптен сенімді болса – онда ол өзін жаңа қолданушы ретінде таныстырып барлығын басынан түсіндіріп көрсетуді сұрауы жеткілікті болды. Компьютерлердің пайда болуымен көптеген фрэйкерлер компьютерлік желілерге ауысып, хакерлерге айналды. Жаңа саладағы SI дағдылары бұдан да пайдалы болды. Егер бұрын корпоративті каталогтардан ақпарат алу үшін операторды шатастырып мазақ қылса, енді жабық жүйеге кіру үшін парольді тауып, сол каталогтардан немесе сол жерден құпия нәрсені жүктей алатын мүмкіндіктер туды. Сонымен қатар, бұл әдіс техникалық қарағанда тезірек және жеңіл болды. Күрделі қорғаныс жүйесіндегі тесіктерді іздеудің қажеті жоқ, Jack the Ripper дұрыс парольді тапқанша күтудің қажеті жоқ, әкімшімен мысық пен тышқан ойнаудың қажеті жоқ. Бар болғаны телефон арқылы қоңырау шалып дұрыс тәсіл қолдану жеткілікті, егер барлығын дұрыс жасасаң оператордан қалаған ақапаратты аласың.

2005 жылдың ақпан айының басында әлемдегі көптеген ақпараттық қауіпсіздік мамандары әйгілі хакер К.Митниктің әлеуметтік инженерияның зияны және әлеуметтік инженерлер қандай әдістерді қолданатыны туралы баяндамасын естіді бірақ өздерін қанағаттандыратындай жауап алмады. Митник тек әлеуметтік инженерияның негізгі ережелері туралы және қылмыскерлер әлеуметтік инженерлік әдістерді құпия ақпарат алу үшін қолданатынын айтты.

Әлеуметтік инженерияны сонымен қатар заңды мақсаттар үшін, ақпарат алу үшін ғана емес, белгілі бір адамның әрекеттерін орындау үшін де қолдануға болады. Бүгінгі таңда әлеуметтік инженерия құпия ақпаратты немесе құндылығы бар ақпаратты алу үшін Интернетте жиі қолданылады сол сияқты қол жетімсіз нәтижелерге қол жеткізу және пайдалы істерге алып келетін жағдайда

адамдарды және топтарды програмаллау үшін қолданылады. Өздерінін кіші кәсіпорындарын дамыту мақсатында әйгілі әлеуметтік инженерлер Дэвид Бэннон мен Питер Фостер әлеуметтік инженерияны қолданған.

Әлеуметтік инженерия тұжырымдамасы жақында пайда болғанына қарамастан, адамдар оның әдістерін ежелден қолдана бастады. Ежелгі Грекия мен Римде адамдар бір-біріне өтірік айтып алдау арқылы жалған ақпаратқа сендіретін болған. Жоғарғы лауазымдылардың атынан сөйлеп, олар дипломатиялық келіссөздер жүргізді, олардың сөздерінде өтірік, жағымпаздық және пайдалы дәлелдер араласып, көбінесе қылыштың көмегінсіз шешілмейтін мәселелерді шешетін. Тыңшылардың арасында әлеуметтік инженерия кеңінен тараған. КГБ мен ЦРУ агенттері өздерін кез-келген адам ретінде таныстырып мемлекеттік құпияларды біле алатын болған.

Әлеуметтік инженерия - қолданбалы әлеуметтік ғылымдардағы бағытталған жиынтық.

Жиынтық бағыттары:

- адамдардың мінез-құлқы мен көзқарасын өзгерту;
- әлеуметтік мәселелерді шешуге;
- әлеуметтік институттардың өзгеретін жағдайларға бейімделуі;
- әлеуметтік белсенділікті сақтау.

1.3 Әлеуметтік инженерияның қолдану салалары, мақсаттары

1.3.1 Жеке адамдарға әлеуметтік инженерия

Шабуылшы сізден белгілі бір мөлшерде ақша алуы керек. Ол сіздің ұялы телефоныңызды және әлеуметтік желіңізді тапты делік және ол сіздің ағаңыз бар екенін біледі, сонымен қатар оның әлеуметтік желісін тауып, оның ой-пікіріне ену үшін оны зерттей бастады. Ол сақтандыру үшін ұялы телефонын тауып, сізбен хабарламалар табатын хат-хабарларды ашты. Ол оларды зерттеп, сіз туралы әртүрлі жеке деректерді тапты, бұл сіздің әлеуметтік желілерді көргеннен кейін оның білімін толықтырды. Келесіде жоспар құрылды, оған мыналар кірді: шабуылдаушы саған кешке қоңырау шалып, сенің ағаң болғандай болып көрінеді, олар оның басын сындырып, көшеде лақтырып тастағанын, телефон мен барлық ақшаны карточкамен ұрланғанын айтады бөтен номермен хабарласқаны да бұған дәлел болады. Сіздің атыңызбен емес, жеке хатында көрген лақаппен сөйлегені өте маңызды - бұл өте маңызды сәт. Әрі қарай, сенімділік үшін ол, мысалы, сіз танитын ортақ достарыңызбен сіз жиі баратын жерде - барда, клубта отырғанын айтады. Одан әрі, мұндай оқиғадан кейін ол ата-аналар үшін ең бастысы - айтпау! Әкемнің жүрегі ауырады (бұзылған диалогтан білді). Осыдан кейін: Маған ауруханаға дейін таксиге 500 р сұрайды, және ол оған көмектескен мейірімді қыз болғанын айтып, карта нөмірін береді,

бірақ оның ақшасы жоқ, бірақ карта бар. Осындай құзыретті тәсілден кейін 10 жағдайдың 8-інде біздің ойдан шығарылған әпкеміз ақша аударады, содан кейін оның ақшасы тек 500р емес, оның шотынан барлық алынады. Техникалық сауатты бұзушы үшін бұл қиын шаруа емес.

Осы алдаудың құпиясын ашайық , шындығына келгенде «бұл әпке» ойдан алынбаған, бұл жағдай шынымен де осыдан 3 жыл бұрын бір қыздың басынан өткен. Оның шотынан 500 р+22000р ұрланған. Бұл жағдайда кейбір нәрселер біртүрлі көрінуі мүмкін мысалы, ол қыз неге ағасының дауысын танымады? Өздеріңіз ойлаңыздаршы түн ішінде эмоцияға беріліп және өзге дыбыстар естіліп тұрса, онымен қоса әпкеміз осы кезде ұйықтап жатқан болатын ал ұйқылы-ояу дауысты ажырату қиынға түседі. Тағы бір ойландыратын жері неге ол қыз ағасының достарына хабарласпастан бірден ақшаны бөтен шотқа салып жіберді. Бәрі өте қарапайым өзіңізді сол қыздың орнына қойып көріңізші, түн ішінде сізге қоңырау келді және ағаңыз екеуіңіз білетін фактыларды дәлме-дәл айтады + ағаңыз сізге өте қымбат жан. Жақсы аналитикалық жұмыс жасап барлығын ойдағыдай істесең адамды эмоцияға берілдіріп логикалық ойлауына кедергі келтіруге болады, бұл жағадай дәл осылай іске асқан. Неге онда осылай алдаудың 10-8 емес, 10-10 іске аспайды. Себебі ағасы әлеуметтік желідегі аккаунтының бұзылғанын біліп қоюы мүмкін, бірақ бұл жағдайда уақыт рөл ойнап тұр. Шабуылшы оны түнде аккаунтын бұзды, ол кезде ағасы ұйықтап жатқан болатын. Жәбірленуші ағасының әйеліне ақшаны аударғаннан кейін хабарласты, себебі ағасы ешкімге айтпауын өтінген болатын, бірақ эмоцияға берілген қыз сонда да ағасының әйеліне хабарласты, ағасының аман-есен ұйықтап жатқанын естіді, және сол кезде алданып қалғанын түсінді.

Тағы бір қызықты мысал - жұмыс логині мен паролін қалай қауіпсіз алуға болатындығы. Жүйелік әкімші жексенбі күні таңертеңгі сағат 8-де жұмыстан қоңырау шалып, былай дейді: «Тыңдаңыз, бізде бұл жерде техникалық жұмыс бар, бла бла бла, әртүрлі қиын шарттар жиынтығы ... сіз келе аласыз ба? Сіз өзіңіздің компьютеріңізді ашуыңыз керек ». Сіз бірден өзіңізге: «жексенбі күні таңертең жұмысқа 1 минутқа кіріп, логин мен парольді енгізіңіз бе ?!» деп ойлайсыз. Бірден сіз: «Басқа нұсқа бар ма?» Деп сұрайсыз. «Әрине бар! Логин мен пароль қажет. Мен барлық мәселелерді шешемін, ал дүйсенбіде сіздің логиндеріңіз бен парольдеріңіз өзгертеміз. » Сіз қуанышты және қуаныштысыз, «жүйелік әкімшіге» құпия сөзбен логиніңізді беріп, ұйықтайсыз. Бұған сенбеңіз, бірақ адамдардың 70% -дан астамы мұны істейді. Яғни, егер әлеуметтік инженер 10 адамды тапса. әр түрлі компанияларда болады және оларды шақырады, содан кейін олардың 6-7-і міндетті түрде оған парольдерін береді. Мұның себептері өте қарапайым: біріншіден, хакер барлық жаман жағдайларды жасайды - таңертең 8-

де, жексенбіде шұғыл, үнемі шақырады. Сіз қайтадан баруыңыз керек екенін дәлелдедіңіз ... және қайтадан, және олар сізге мәселенің қарапайым шешімі түрінде жеңілдік береді! Әрине, көпшілік келіседі. Бұл әсер ету механизмі сіз алдымен қандай да бір проблеманы шешіп, содан кейін біраз уақыттан кейін шешім қабылдаған кезде контраст принципі деп аталады.

1.3.2 Коммерциялық ұйымдарға әлеуметтік инженерия

Әлеуметтік инженерия интернетте құнды ақпарат алудың психологиялық әдістеріне сілтеме жасау үшін қолданылады. Көбінесе - құпия мәліметтерді ұрлап немесе қажет әрекеттерді жасайтындар киберқылмыскерлер. Соңғы екі жылда әлеуметтік инжинирингтің көмегімен жүз банктен 2 миллиард доллар ұрланған. Алайда, әлеуметтік инженерлердің барлығы бірдей алаяқтар емес. Олар бәсекелестердің шабуылынан немесе қара пиардан кейін компанияның жақсы атын қайтара алады. Психологиялық әдістер, мысалы, анонимді комментатордың мәліметтерін алу үшін және оны қажетсіз пікірлер мен жала жабудан арылту үшінде қолданылады. Әлеуметтік инженерлер форумдарда тіркеліп, теріс пікірде болған аудиториямен әңгімелесуге қатысады және оның пікіріне нейрингвистикалық бағдарламалау әдістері әсер етеді.

Бірінші жағдай. Қызметте емес, достықта

2007 жылы әлемдегі ең қымбат қауіпсіздік жүйелерінің бірі бұзылды. Зорлық-зомбылықсыз, қарусыз, электронды құрылғыларсыз. Ер адам өзінің күшімен Бельгияның ABN AMRO банкінен 28 миллион доллар алмаз алды. Алаяқтықтан бір жыл бұрын Израильде аргентиналық паспорты ұрланған ер адам Карлос Хектор Фломенбаум банк қызметкерлерінің сеніміне ие болды. Өзін кәсіпкер ретінде көрсетіп, суретке түсіп, шоколад берді. Бірде қызметкерлер оған 120 000 каратқа бағаланған асыл тастардың жасырын қоймасына кіруге рұқсат берді. Кейін бұл іс жоғары дәрежелі тонаулардың бірі ретінде танылды.

Әңгімнің моральдық мәні: технологияның қандай түрі қолданылсада және қаншалықты қымбатқа түсетініне қарамастан - адам факторы болған кезде жүйе осал.

Көбінесе, жоғарыдағы мысалдағыдай, әлеуметтік инженер «құрбан болғандардың» сенімін арттырып, оларды басқарудың қажеті жоқ. Барлығына көрінетін ақпаратты дұрыс пайдалану үшін жеткілікті заттар: жұмыс үстеліндегі пошта, телефон экранындағы ескертулер немесе қоқыс. Әлеуметтік инженер адамдарға қысым жасамай-ақ мәліметтер ала алады.

Екінші жағдай. Жай ғана сұраңыз

2015 жылы Ubiquiti Networks 40 миллион долларды ұрлап кеткен. Ешқандай операциялық жүйелер бұзылған жоқ. Ешкім деректерді ұрламады. Қауіпсіздік ережелерін қызметкерлердің өздері бұзған.

Алаяқтар компанияның топ-менеджерінің атынан электронды хат жолдады. Олар жай ғана қаржыгерлерден көрсетілген банктік шотқа үлкен соманы аударуды өтінді. Әлеуметтік инженерияның бұл әдісі адамның әлсіздіктеріне әсер етеді. Мәселен, өзінен жоғарғы биліктегі адамдарға жағу үшін және қызмет ету ниеті.

Психологтар эксперимент жүргізді (толығырақ Роберт Чалдинидің «Әсер ету психологиясы» кітабын қараңыз, 2009 ж.). Бас дәрігердің атынан олар медбикелерді шақырып, науқасқа дәрінің өлім дозасын салуды бұйырды. Әрине, медбикелер өздерінің не істегендерін білді, бірақ 95% жағдайда олар бұйрықты орындады (зерттеу авторлары оны палатаның кіреберісінде тоқтатты). Алайда олар дәрігердің жеке басын растауға тырыспады. Неліктен медбикелер мұны жасады? Билікке бағыну. Дәл осындай жағдай Ubiquiti хикаясында да болды.

Үшінші жағдай. Уолл-стритті дүр сілкіндірген сөйлем

2013 жылдың сәуірінде The Associated Press ақпараттық агенттігінің Twitter-дегі парақшасында жаһандық экономикаға ауыр соққы болған жалған твит пайда болды.

1.3 – сурет. Аудармасы «Шұғыл: Ақ үйдегі екі жарылыс, Барак Обама жарақат алды»

Осы жаңалықтарда қор индекстері құлдырады. Ақ үй бұл хабарды жоққа шығарғаннан кейін жағдай қалпына келді.

Есептік жазбаны бұзғаны үшін жауапкершілікті Сирияның Электрондық армиясы өз мойнына алды. Бұған дейін АР қызметкерлерінің бірінің атынан хакерлер өз әріптестеріне өте маңызды сілтемені басуды сұрап «хаттар» жіберіп отырғаны хабарланды. Онда пайдаланушыдан логин мен парольді енгізу арқылы кіру сұралды. Сонымен, шабуыл жасағандар редакция қызметкерлерінің жеке шоты туралы мәліметтер алғысы келді.

Бұл жағдай осындай кибершабуылдарға қарсы осалдығымызды көрсетеді. Бүгін бұл The Associated Press, ал ертең беделге нұқсан келтіретін вирустық хабарлама жіберетін кез-келген компания болуы мүмкін.

Қылмыскерлер жаңа схемаларды әзірлеуде - оларды салық инспекторлары ұсынады және «қарызды төлеуге» ақша талап етеді, немесе оларды банк қызметкерлері ұсынады және PIN-код талап етеді.

Қауіпсіздіктің кез-келген ерекшеліктері (антивирустар, брандмауэр) сізді осындай шабуылдардан құтқара алмайды. Қауіпсіздік саясатының әртүрлі нұсқаларын жасау, пайдаланушыларды оқыту, компания ішіндегі құрылғыларды пайдалану ережелерін анықтау маңызды. Сондай-ақ қауіптің болуы туралы ескерту жүйесін жасаңыз, техникалық қолдау үшін жауапты адамдарды белгілеңіз және қос тексеруді ұйымдастырыңыз.

Коммерциялық ұйымдардан дерек қорларын ұрлау.

Кім қандай жолмен ұрлайды?

Оны қарапайым адамдар, көп жағдайда күрделі құралдарсыз, USB портқа қосылған Flash Drive қарапайым жинақтауышты қолданып ұрлауы толық мүмкін.

Жоғарыда айтып кеткендей, 100-дің 80 жағдайында ақпаратты техникалық арналар емес, әлеуметтік арналар арқылы ұрлайды.

Мысалы:

-Ренжулі жүйелік адаминистратор өзімен бірге ДҚ–н, кәсіпорын туралы барлық ақпаратты алып кетеді;

-Белгілі бір төлем үшін компания қызметкері ұрлайды;

-Бөтен адам сол жүйедегі жүйелік администратордың жақын досы боп, келеді (жүйелік администратор досы сол күші ауырып қалды) және т.с.с..

Әлеуметтік арна арқылы ақпараттың ұрлануы, АҚ тапсырмасы өте қиындатып жібереді.

Кәсіпорында:

-Техникалық арна арқылы ақпараттың сыртқа шығып кетуі.

-Желі қорғалған, сырттан ешқандай шабуыл келе алмайды.

-Керек десең, мекеменің ішкі желісі сыртқымен байланыспайды (Ресейдегі күш құрылымдарында интернетке шығыс жоқ).

-Маңызды кеңестер өтетін кабинеттер Ақпаратты Қорғау жабдықтарымен жабдықталған;

-Диктофондар орнатылған;

-Радиоарналар, көлденең электромагниттік сәуле арналары үшін радиошуыл генераторы қойылған;

-Виброакустикалық арна жабық, әйнек терезесінің тербелісі арқылы ақпаратты лазерлік түсіру және тыңдау мүмкін емес, олар қорғалған.

Бірақ ақпарат шығып кетті.

Оны адам алып кетті. Бұл ақпараттың негізінен адам арқылы сыртқа кететініне дәлел.

АҚ–ға байланысты мұнай–химия саласының ірі компаниясына аудит жүргізілген. (ірі милл. $ обороты бар?)

Директордың хатшысының үстеліне кім тиіскен деп ойлайсыз?

-Түнгі кезектегі кіші қызметкер.

- Компанияның 5 жылдық даму жоспар;
- Сырттан келген хаттар;
- Компанияның шешімдері.

Тағы бір әлеуметтік инженерия арна – түрлі көрмелер, презентациялар және т.б.

Ақпараттық қауіпсіздікте - жүйелік болу керек, яғни барлық жағынан қорғалу керек.

Ақпараттық қауіпсіздікте «жүйесіздік» деген не?

-Адамдардың жалақысы төмен;

-Атқарған жұмысын жек көреді;

-Директордың алдында кезекте көп күтіп калады;

-Директорға өкпелі;

-Директор айқайлап, сөйлейді, қабылдауында күтіп отырғандар оның айтқанын естіп жатыр

және т.с.с..

1.3.3 Әлеуметтік инженерияны күнделікті ақша табу жолында қолдану.

Әлеуметтік инженерия көптеген кітаптарда жазылғандай ақпаратты бұзу мен алу үшін ғана емес, сонымен қатар нақты жағдайларда қарапайым пайда табу үшін де қолданылады. Күнделікті өмірде біз компьютерлер мен қызметтерді бұзбаймыз, бірақ күн сайын ақша табуымыз керек.

Біз әлемде ең көп таралған мысалды талдаймыз. Бір компания бар, коды фирмалық нөмірі №1. Кез-келген жақсы компаниялар сияқты, оның сол өнім немесе қызмет ұсынылатын көптеген сайттары бар. Сайтқа кірушілердің негізгі көзі болып табылатын іздеу жүйелері көп келушілерді алу үшін белгілі бір сұраныстың берілуін әр түрлі етіп жасауға тырысады , сондай-ақ ақша табу үшінде. Бұрын сол компания 10-нан 50-ге дейін сайт құрып, олардың барлығын

нәтижелерінде бірінші және екінші параққа шығаруға тырысты. Нәтижесінде, адам қай сайтты таңдағанына қарамастан, сол компанияға бірдей тапсырыспен жүгінді. Уақыт өте келе бұндай тәсілдер азая бастады , себебі іздеу іздеу жүйелері арнайы фильтрларды қолдана бастады. Егер компанияның мақсаты тауарларды сату және қызмет көрсету болып табылса және сол үшін әртүрлі сайттар мен әртүрлі сұрансытарды қолданса фильтр тек бір сайтты ғана қалдырады. Енді сол фильтрге қарсы тұру үшін көптеген әдістер ойлап табылды, олардың біреуі домен иесінің деректерін whois өтініші бойынша жасырады.

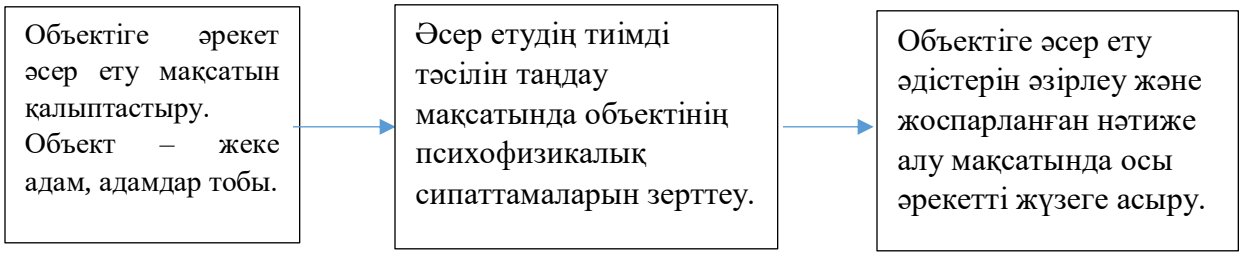
Әлеуметтік инженерия тек алдау үшін ғана емес, статистика әдісі ретінде де қолданылады. Мысалы, сайт қымбат көліктерді сатады. Тауардың астында бірнеше каналды телефон мен қолтаңба бар, «өзіңіздің жеке менеджеріңізден сұраңыз». Тағы бір өнім бойынша - «Александр менеджерден сұраңыз» және т.б.

Белгілі бір беттерден немесе сайттардан келген қонақтардың қоңырауларының статистикасын дәл жүргізу үшін осы ұйымда мүлдем жұмыс жасамайтын адамдардың аттарын көрсету ұсынылады. Шындығында мұндай адамдар тіпті жоқ, және барлық қоңырауларды бір немесе екі адам өңдей алады. Бірақ мұндай қолтаңбалар ұйымға беріктік береді, сенім деңгейін арттырады және маркетинг мақсатында қолданылады.

2. Әлеуметтік инженерия қарулары

2.1 Әлеуметтік программалау.

Әлеуметтік программалауды мінез-құлқын дұрыс бағытта өзгерту немесе сақтау мақсатында адамға немесе адамдар тобына бағытталған әсер етуді қарастыратын қолданбалы тәртіп деп атауға болады.Әлеуметтік программалаудың негізгі тұжырымдамасы адамдардың көптеген әрекеттері және олардың белгілі бір сыртқы әсерге реакциясы көптеген жағдайларда алдын-ала болжануы болып табылады. Әлеуметтік программист адамдарды басқару өнерін меңгеруді мақсат тұтады.



Сурет -2.1. Әлеуметтік программистердің жұмыс әдісінің жалпы сұлбасы

Мысалы: орынбасарына бастық өте кедергі болады. Айталық, орынбасар бастықтың жүрегі ауыратынын біледі, бастық арақ ішкенді жақсы көреді. Бірақ туыстары оған ішкізбей, үнемі аңдып, денсаулығын қадағалап жүреді. Ал орынбасар бастықтың осы әлсіз жерін басып, оны қандай жолмен болса да ішкізеді. Бастық Геморрагический инсульт алады, өледі. Орынбасар бастықтың орнына отырады. Жерлеуде бәрінен көп жылаған осы орынбасар болады...

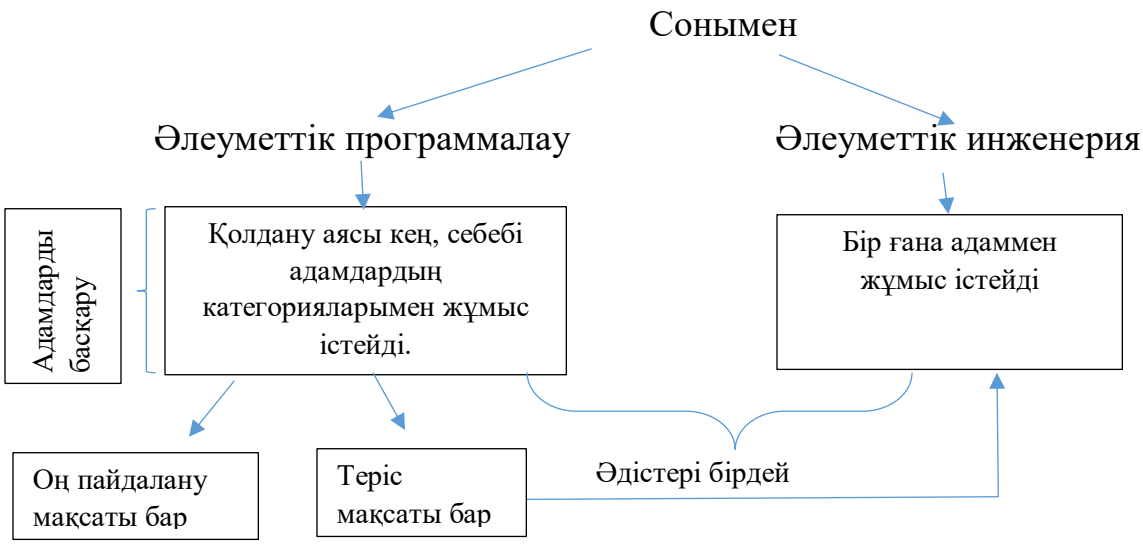
Әлеуметтік программалау әдісінің жақсы жері:

- Қылмыскерді ешкім білмейді;
- Білгеннің өзінде жауапқа тарта алмайды;
- Инсультқа дейін жеткізді деген статья жоқ. Болғанның өзінде дәлелдеу өте қиын.

Сурет – 2.2. Әлеуметтік инженерия процесі

Әлеуметтік программалау мынадай психологиялық концепцияларға негізделеді.

- Трансактілі талдау
- Әлеуметтану (адамдардың топтағы мінез–құлқы туралы ғылым)
- Нейролингвистикалық программалау
- Сценарийлік программалау
- Психологиялық типология



Сурет – 2.3. Әлеуметтік инженерия және әлеуметтік программалауды түйісу сұлбасы

Әлеуметтік программалауға мысал.

Атақты гроссмейстерге почтадан хат алады. Оған жас шахматшы «шахмат ойнайық» деп ұсыныс тастайды, дистанциядан. Жүрістері почта арқылы беріледі. Егер ұтса гроссмейстерге үлкен көлемде ақша төленетін болады. Тең түссе немесе ұтылса, жас шахматшыға ақша төленеді(екі есе аз). Екеуі келіседі. Алғашқы жүрістен–ақ ол перспективті шебердің жүрісін байқайды. Матчтың жартысында гроссмейстер ұйқыдан қалады, алдағы жүрістерді ойлап, басы қатады. Соңында екеуі тең түседі. Сөйтіп ол жас шахматшыны мақтап, қолдау білдіріп, чемпион қыламын дейді. Ол қолдауынан бас тартып, ақша сұрайды. Гроссмейстер төлейді.

Себеп: Гроссмейстермен басқа ұлы Гроссмейстер ойнайды. Оған да жас шахматшы хат жазған. Ол да келіскен. Екеуінен де ақша сындырады. Нәтижесінде жарты жыл бір–бірімен шайқасқан ұлы гроссмейстерлер алаяққа жем болды. Ол жас шахматшы – почталық ретрансиятор қызметін атқарды, бірінің хатын біріне жіберіп отырды.

Әлеуметтік инженерияның қолданудың негізгі облыстары төмендегі суретте берілген.

Сурет- 2.4. Әлеуметтік инженерияның қолданылу салалары

Әлеуметтік программалаудың психологиялық негіздері

Неге көптеген адамдар әлеуметтік хакерлердің жемтігіне айналады? Себебі 90% адамдар автопилотта өмір сүреді. «біздің борттық компьютерімізде» мінез–құлықтың бірнеше модельдері (программалары) бар, біз уақытқа байланысты осы күйлерге ауысып тұрамыз. Түскен сигнал,а байланысты әрекет етеміз. «Өрт» десе, қашу керек деп тұрасың.

Нәтиже не? Адамдар өмірінің көп уақытын «автопилот» режимінде (программалар әлемінде) өткізеді. Кейде ғана «қолмен басқару» режиміне көшеді. Ситуацияға стериотипті әрекет етеді.

кеменің бататынына көздері жетсе де әрекет етпеген команда суға кеткен

инструктор көлін жүргізуді үйретіп жүр. Машинада екі тормоз бар. Екеуі де тормозда, баспай апат болды

«Өзара көмек» программасы

Біреудің машинасын ұрлап мініп бара жатқан ұры жолда машинасы бұзылып тұрған кызға тоқтап, көмектесті. Телефон алмасып жөніне кетті. Біршама уақыттан кейін қыздан көлігін бір жерге барып келуге сұрады. Ол берді, көлігінен біржола айырылды.

Қазір автосақтандыру деген бар, бұл алаяқтықты көп іске асыра бермейді

Әлеуметтік еліктеу программасы

Бұл программаны әлемеуттік хакерлер адамдарға жақсы қолданады. Адам өзге адамдардың «дұрыс» дегенін дұрыс деп санайды.

Мысалдар:

Клакерлер – көрермендерге қажет реакция беретін, арнайы шақырылған қолшапалақтаушылар.

Кезек қалыптастыру тауар өту үшін, сол жерге кезек ұйымдастырылады. (Адамдар мына жерде неге очередь, значит күшті деп ойлайды).

Трассадағы кептеліс. Кептелісті айналып өтпек болып, бір машина қарсы жолға шығып кетеді. Оның артынан 5-6 шопыр кетеді.

1969 жыл үш американдық психолог эксперимент жасаған. Олар орталық көшеге шығып, жоғары қарап тұрған. Айналасына адамдар жиналып, олар да аспанға қарап тұрған

араб елдерінде адамды таспен ұрып, жабылып өлтіру

Банкті банкрот қылудың бір тәсілі: банк жанына көп адам жиналып қалады. Ақшаларын шешіп алмақшы(өтірік қой). Оны өтіп бара жатқандар көреді. Әлеуметтік желіге түсіріп, жібереді. Барлық салымшылар лап қояды, елдер осылай істеп жатыр екен деп.

2.2 Претекстинг

Претекстинг (сценарий) – алдын ала анықталған әрекеттер жиыны, нәтижесінде құрбан қандай да бір ақпаратты береді немесе белгілі бір әрекетті орындайды.

Бұл әдіс клиент туралы ақпаратты ашу (туған күні, әлеуметтік сақтандыру көмір, шоттарды соңғы сомасы және т. б.), үшін қолданылады, ол үшін

–телефондық әңгімені жазып алу;

–пайдалы отчеттар, банк отчеттары алу (тікелей компания өкілдерінен) көзделеді.

Мысалы, онлайн–мессенджер бойынша шабуыл.

Бұл схемада алаяқтар телефон иесімен не SMS арқылы байланысып, одан алдын-ала дайындалған сценарий бойынша оның картасындағы деректерді алаяқтық жолмен біледі. Сондықтан әдіс претекстинг деп аталады (ағылшынша pre-text, предварительный текст): алаяқ алдын ала дайындалған мәтінді барлық психологиялық тұзақтармен айтады. Бұл келесідей көрінуі мүмкін: шабуылдаушы сізді банк қызметкері ретінде таныстырып, сіздің картаңыздан санкцияланбаған төлем жасалғанын немесе сіздің картаңыз бұғатталғанын, немесе сізде қарызыңыз бар деп мәлімдейді және сол сияқты, егжей-тегжейлер көрсетілмейді және сізден құпия ақпарат беруіңізді сұрайды бұл мәселені шешу үшін сіздің картаңызға (PIN, CVV коды және т.б.)

Бұл қорқынышты үнемдеудің жалпы әсер ету үлгісі. Қаржы қауіпсіздігіне қауіп туралы күтпеген жаңалықтар (мүмкін қаражатты есептен шығару, картаны оқшаулау) жәбірленушіні күшті эмоционалды күйге келтіреді (мазасыздық, қорқыныш), бұл жағдайды сабырлы түрде талдауды қиындатады.

Дәл осының салдарынан зардап шегушілер жиі қателеседі - «құтқарылу» үшін олар айтылғанды ойланбастан жасайды және банк қызметкерлері PIN немесе CVV кодын сұрай алмайтын жад бұғатталады. Сонымен қатар, банк қызметкерлері жиі-жиі SMS растауынан кодты енгізуді немесе атауды сұрайды - бұл тек банкке барғанда ғана емес, клиент байланыс орталығына немесе қолдау чатына қоңырау шалғанда да. Нәтижесінде, адамдар банк қызметкеріне SMS-тегі кодтар туралы хабарлау қалыпты және қауіпсіз деген ойды қалыптастырады. Бұл стратегиясы құпия деректерді «анықтауға» негізделген алаяқтардың жұмысын жеңілдетеді. Жәбірленушінің ақшасын картада алуға мүмкіндік беретін осы құнды ақпарат техникалық құралдармен танылмайды, бірақ психологиялық айла-шарғы жасау арқылы адамның қолына түседі. Мұны әлеуметтік инженерия деп атайды.

2.3 Фишинг

Қолданушылардың құпия деректеріне рұқсатсыз қол жеткізу мүмкіндігін алу мақсатындағы интернеттегі алаяқтың түрлерінің бірі.

2013 жылы электрондық почта арқылы жіберілген 509 хаттан 1-ші фишингтік хат болған. 1фишингтік шабуылдың өзіндік құны 2000$-ға дейін жетеді, ал пайда 10000$-ға дейін жетеді.

Фишерлер жалған электрондық хаттарды қолданады.

Мысалы: банктің атынан жіберіп, парольді растауды сұрауы нмесе ірі көлемде ақша аудару туралы білдіріс (уведомление) жіберуі мүмкін. Құрбан фишердің алдауына оңай түседі, өз еркімен және деректерін бере салады.
Олар жақсы психологтар, әрекеттері – нақты.

Фишингтің негізгі 3 түрі бар:

-почталық

-онлайндық

-аралас.

Почталық: қандай да бір құпия деректі сұрап электрондық хат жіберіледі.

Мысалы: почталық адресі ұқсас интернет – провайдер атынан база «бұзылды», сол себепті сіздің логиніңіз бен пароліңіз керек, – деген сияқты.

Онлайн: Алаяқ қандай да бір танымал сайттардың бірінің дәл көшірмесін алады, және де ол үшін өте ұқсас домендік ат таңдалынады (немесе сол домендік ат, бірақ басқа зонада), осылайша ұқсас дизайн құрылады.

Мысалы, интернет-дүкен. Бағасы өте арзан. Сатып алу үшін қолданушы логин, пароль және пластикалық картасының нөмірін енгізеді. Бұл сан сәтте алаяқтың қолына түседі, карточканы босатады.

Аралас-фишинг: Алдыңғы еке бірге қолданылады.

Олар жеке-жеке қолданыла алмайтын болды, қолданушыларды алдау қиынға соқты. Онлайндық фишингтегі сияқты жасанды сайт құрылады, сонан соң почталық фишингтегі сияқты осы сайтқа кіруді сұрайтын хат жіберіледі. Мұнда қолданушылардан құпия деректері сұралмайды, тек сайтқа кіруін сұрайды. Қалған істі өздері тындырады

Фишерлер белгілі бір оқиғаларды жақсы пайдаланады. Мысалы: туған күнімен құттықтап ашық хат келеді:

«Туған күн» акциясының шеңберінде өзі клиент болып табылатын банк оған 500$ аударып, туған күнімен құттықтайды, - деген, алу үшін: банк сайтына (әрине, жасанды сайт) кіріп, қажетті ақпаратты енгізуді сұрайды.

Қазір дүниежүзі бойынша IT- мамандар түрлі тәсілдерді әзірлеуде. Браузерлерде фишинг-сайттардың қара-тізімі құрылады.

Ұсынылған әдістер:

-бір реттік парольдер генераторлары;

Фишинг маңызы – парольдер мен банк мәліметтерін алу болғандықтан, генератор осы алаяқтықтың жолын кеседі. Генератор – шағын калькулятор сияқты. Қолданушы банк сайтына кірген кезде, өз шотына қатынас алу үшін генератор көрсететін символдар тізбегін енгізу керек. Банк те пароль құру үшін генератордағыдай алгоритмді қолданады. Екі пароль сәйкес келгенде, қатынас

ашылады. Мұндай парольді ұрлау мүмкін емес, себеп ол 1-ақ рет қолданады. Кемшілігі – клиент үшін қосымша шығын.

Қазіргі уақытта АҚШ, Еуропаның көпетеген банктері, сондай-ақ ірі интернет-провайдерлер осындай бір реттік парольді қолданады (мысалы, провайдер AOL)*/

-USB-құрылғылар қолдану

Қолданушы өз компьютеріне USB-құрылғы қоспайынша, өз щотына қатынас ала алмайды. Алаяқтар үшін қолданушы есепшоты қолжетімсіз.

-Мобильдік тұжырымдау (подтверждение)

Қолданушы өзінің ұялы телефонынан (банкке белгілі нөмір телефоны) қандай да бір SMS жіберген соң ғана картаға қатынас ашылады.

-Нақты Web-сайттың парольдерін хештеу

/*Пароль қолданылатын сайт үшін парольге ерекше информация қосу арқылы құпия деректерді ұрлаудың болдырмау үшін парольдерді хештеу. Қолданушы арнайы формада өз паролін енгізеді, ал браузер оны түрлендіреді және қажетті ақпаратты қосады. Қолданушы пароль енгізетін Web-сайтқа бұл пароль таза түрде хабарланбайды, сайтқа хештелген пароль келеді. Осылайша, қолданушы лақап сайтты өз паролін енгізгенімен, хакерлер оны қолдана алмайды. Нағыз рас сайтты хештеудің қолданушы картасындағыдай схемасы қолданады*/.

Фишингтің жиі кездесетін қолданыстағы түрлері:

-Қолданушыға қандай да бір қызмет немесе мүмкіндік ұсыну, мысалы ВКонтактеда және парақшаға кімнің кіргненін білуді ұсыну (бұл мүмкіндік ВК-да жоқ);

-Сайтта авторизацияны тексеру;

-Электрондық почтада спамнан құтылу (отписаться) қажеттілігі;

-Арзан бағада сауда-саттық жасау;

-Жаңа қосымша орнату қажеттілігі;

-Әлеуметтік желіде (мысалы, Facebook) бір ұйымның корпоративті парақшасына лайк(лүпіл) қою.

/*ауысша тегін кофе ұсынады, ол кофесіне тапсырыс беріп жатқанда, ол туралы және деректері ұрлайды; туған күні, ата-анасына ата-жөні білімі, және т.б. осының бәрі бір ғана лайктың арқасында*/

-Интернет-аукциондар өткізу (өз істерін легальді аукционды жүзеге асыруды, бірақ түскен қарсы жалған веб-түйінмен аударылады).

-Қайырымдылық ұйымдарының атынан шығу.

-Фишингтік интернет-дүкендер

Фишингті қалай тануға болды?

-Лотореядан ұтқандығы, үлкен жүлде күтіп тұрғандағы жөнінде хат түсу (авторизацияны бөгде ресурсқа және аккаунттың деректері кетіп қалады);

-Арзан бағада зат ұсыну, карта (кредиттік карта номірін, аты-жөнін, картаның жарамдылық мерзімін, құпия кодын CVV енгізуінен кейін) карта арқылы төлем жасауды сұрайды, ақпарат сол сәтте қаскүнемге түседі.

-Фишингтік сайттар қалқып шығатын терезелер артында жасырынып тұруы мүмкін. Оған таргеттелген жарнама енгізуі мүмкін (бапталатын, онлайн-жарнама).

/*Қолданушы «логин» графасында өзінің электрондық почтасының адресін көру мүмкін болатын жағдай. Кездеседі, оған төменгі графада паролін енгізу жөнінде ұсыныс түседі. Ондай ұсыныс өзіңнің досыңнан түсуі мүмкін (оның аккаунты бұзылды деген сөз)*/

Фишингтен қалай қорғануға болады?

1)Банк картасының пин-коды, электрондық почта паролі, әлеуметтік желідегі аккаунттар паролі сияқты құпия деректерді ешқашан, ешкімге бермеу керек (банк та, әлеіметтік желі де, электрондық почта арқылы мұндай деректер сұрамайды).

2) Антивирустардың соңғы базасын қамтитын жақсы антивирус орнату. Соңғы заманауи антивирустарда шпиондық және зиянкес программалардан қорғау мүмкіндіктері қамтылған. Әлеуметтік желілер мен браузерлер де күдікті сайт туралы қолданушыға ескертіп отырады. Оны елеусіз қалдыруға болмайды. Егер әлеуметтік желі сілтеме бойынша өтпеу керек десе, таңдау керек. Егер сіздің электрондық почтаңыз хатты спам ретінде белгілесе, яғни оған себеп бар.

3) Сайт дизайнына үнемі көңіл бөлу керек. Егер сайт немесе лендинг (мақсатты сайт-контекстік реклама қамтиды, бір ғана қызмет түрін ұсыну керек. 5 түрлі өнім үшін 1 лендинг құруға болмайды. Әр өнім үшін жеке парақша құрған дұрыс.) күдік тудыратындай болса, онда ол фишингтік сайт.

4)Ауысу сілтемесіндегі адрестік қатарға көңіл аударыңыз. Электрондық адрестегі елеусіз өзгерістер сізді басқа сайтқа лақтыруы мүмкін. (мысалы, mail.ru →meil.ru, vk.com→vk.co немесе vka.com).

Сонымен қатар қысқартылған сілтемелерден абай болу керек.(мысалы,bit.by, оның артында жасырынып жатқанын бір қарағанда білу мүмкін емес)

5)Банк сайттарына кірген кезде https қорғалған қосылыстың орнатылғанын қадағалаңыз. Адрестік қатарда арнайы символ – құлып (замок) тұру керек. Осы замокты басып, https үшін сертификатты тексеруге болады.

6)Таныс емес адрестік хаттар, экстремдік сипатқа ие.

-Сіздің аккаунтыңыз бұзылды.

-Сіздің профиліңіз бұғатталады.

-Ірі ұтыс туралы хабарлаймыз.

(осылар көп жағдайда алаяқтық болады).

7) Банк веб-аккаунттарына қоғамдық Wi-Fi қатынас нүктелері арқылы кіруден сақ болу керек. (Мобильді интернетті немесе қорғалған қойшасты қолданған дұрыс одан да).

8) Сізге танымал сияқты бір компаниядан немесе сервистен фишингтік хат келді делік, егер күдігіңіз болса осы компанияның бөлімшесіне хабарласу керек. Компания тиісті шара қолданады. Сонымен осындай сайттың веб-хостинг провайдермен байланысып, жалоб қалдыра аласыз. Көптеген хостерлер осы секілді хабар алған кезде фишингтік веб-сайттарды жазып тастайды. Бұл арқылы сіз басқа қолданушыларға көмектесетін боласыз. (досыңыздан келген күдікті сайтқа да абай болу керек, хакерлер досыңыздың аккаунтын бұзып, сол жерден жіберуі де мүмкін).

2.4 Фарминг

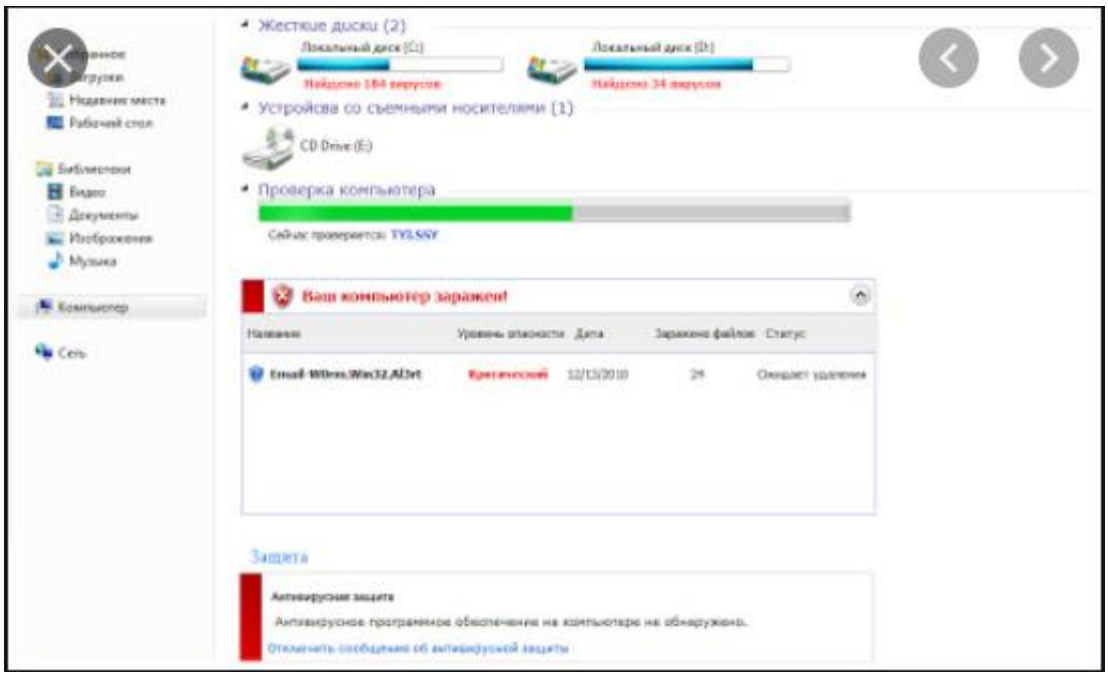
Фишингке қарағанда қауіптірек алаяқтық болып табылады. Мақсаты DNS-адресті өзгерту, нәтижесінде қолданушы түсетін сайт түпнұсқа емес, фишинг бет болып шығады.

Фарминг қолданушыларды алдап сайттарға автоматты түрде қайта бағыттайды. Потенциалды құрбандардың хат жіберіп, жауап күтпейді: ешкім хат жазбайды, сайтқа кіруік сұрамайды. Қолданушы өзі қалап, банк сайтына кіреді. Бірақ бұның жасанды сайт екенін білмейді.

Хакерлер бұл әдісті сәтті қолданады, өйткені бұл бір уақытта көптеген құрылғыларға енуге мүмкіндік береді. Бұдан басқа, олар пайдаланушыларды кез-келген күмәнді түймені басуға, электрондық поштаның немесе жарнаманың сілтемесін басуға сендірудің қажеті жоқ. Оның орнына зиянды код пайдаланушының саналы әрекетінсіз автоматты түрде жүктеледі.

Фарминг қалай жұмыс істейді?

Фарминг жеке компьютерлерге ену немесе серверді жұқтыру нәтижесінде пайда болуы мүмкін. Екі жағдайда да қолданушыны жалған сайттарға бағыттауға мүмкіндік беретін арнайы код қолданылады, бірақ әртүрлі тәсілдермен.



Сурет 2.5. Жалған хабарлама жіберудің бір көрінісі

Дербес компьютерлерге фарминг

Фармингтің бұл түрінде хакер жеке компьютерде хост файлын өзгерте алатын коды бар электрондық поштаны жібереді. Хост файлын өзгерткеннен кейін ол сайттың нақты мекен-жайларын жалған адрестермен алмастырады. Нәтижесінде, егер қолданушы браузерінің мекен-жай жолына дұрыс веб-мекен-жайын енгізсе де, ол әлі де нақты веб-сайтқа ұқсас жалған веб-сайтқа бағытталады, яғни қолданушылар оны байқамай, түсінбеуі мүмкін. алаяқтықтың құрбаны болды.

Фармингтің негізгі екі формасы бар:

1) Потенциалды құрбандардың компьютеріне хакерлер зиянкес ПҚ (прог. Қамт.) орнатады.

Компьютерге кірген вирус автоматты түрде қолданушыны кіргісі келген сайттан автоматты түрде жасанды сайтқа (онлайн бан немесе дүкен) қайта бағыттап жібереді.

2) Өте аяр, бүлдіргіш. DNS серверді жұқтыру, нәтижесінде оның әрбір қолуданушысы алаяқтың сайтқа бағытталған болады.

DNS(Domain Name System) – домендік атаулар жүйесі, домендер аттарын осы домендерге сәйкес келетін компьютерлер IP-адрестерімен байланыстырады

DNS – браузер қолданушы терген сайт адресін осы сайт орналасқан сервердегі нақты IP-адреспен сәйкестендіруге арналған.

DNS қызметін телефон анықтамасымен жиі жиі салыстырады.

Аты таңдалады.

Нөмірге қарайды.

Көрсетілген нөмір бойынша хабарласады.

DNS қызметі

Сайт аты таңдалады

DNS қызметі оның «нөмірін» (IP-адрес) айтады

Көрсетілген сайтқа көшу

Фармингті қалай тануға болады?

Кейде фарминг шабуылын анықтау мүмкін емес, себебі ол қолданушы тарапынан қандай да бір әрекетті білдірмейді. Алайда, сізде ауылшаруашылық шабуылының құрбаны екеніңізді көрсететін бірнеше негізгі ескерту белгілері бар, сондықтан біздің кеңестеріміз:

Браузердің мекен-жай жолындағы сайт адресі (URL) дұрыс терілгеніне көз жеткізіңіз.

URL мекенжайы қауіпсіз және «https» басталатынына көз жеткізіңіз.

Сізді қызықтыратын веб-парақтың көрінісі кез-келген сәйкессіздіктерге назар аударыңыз.

Сіздің банктік шотыңыздағы кез-келген ерекше әрекетті ұмытпаңыз.

Өзіңізді фармингтен қалай қорғауға болады?

Көптеген фарминг шабуылдарының алдын алу іс жүзінде мүмкін болмағанымен, киберқылмыскерлерді тоқтата алатын бірнеше қадам бар:

Егер сіз шабуылдың құрбаны деп ойласаңыз, DNS кэшін жойыңыз.

Құрылғыңыздың қауіпсіз екеніне көз жеткізу үшін антивирустық бағдарламаны іске қосыңыз.

Егер сіздің DNS серверіңіз бұзылды деп ойласаңыз, Интернет-провайдеріңізге хабарласыңыз.

2.5 Трояндық ат

Трояндық ат – қолданушының көрсеқызарлығына, қорқынышына немесе басқа да эмоцияларына негізделеді.

Троян вирусы дегеніміз не?

«Трояндық вирус» термині біршама қате, бірақ әдетте «троян» терминінің орнына қолданылады. Вирус кәдімгі компьютерлік файлдарды жұқтырады - ол бөлек файлды түсіріп алады және оны процесте бұзады немесе зиянды түрде өзгертеді. Содан кейін ол басқа файлдарды жұқтырып, басқа компьютерлерге таратуға тырысады.

Вирустардан айырмашылығы, трояндар - бұл бағдарламалар, олар өздерінің лас жұмыстарын жасау үшін басқа файлда жұмыс істеудің қажеті жоқ. Сонымен қатар, олар өздігінен көбеюге қабілетсіз. Алданбаңыз: трояндардың әрекеттерінің салдары кез-келген компьютерлік вирус сияқты жойқын болуы мүмкін.

Трояндық ат (трояндық вирус) қалай жұмыс істейді?

Ежелгі грек мифологиясындағы трояндық жылқының оқиғасындағыдай, трояндық зиянды бағдарлама қалағанның «кескінінде» пайда болады. Ол өзін ақысыз бағдарлама немесе электрондық поштаның қосымшасы ретінде жасырады, содан кейін компьютерге орнатуға рұқсат берген кезде ол шлюздерді ашады.

Троян компьютерге кіре салысымен, ол кез-келген нәрсені істей алады, бірақ зиянды бағдарламалардың көпшілігі сіздің компьютеріңізді толықтай басқаруға ұмтылады. Басқаша айтқанда, компьютердегі барлық әрекеттеріңіз жазылып, троян көрсеткен серверге жіберіледі. Егер сіз компьютерде қаржылық транзакциялар жасасаңыз, бұл өте қауіпті, себебі троян сіздің картаңыз туралы ақпаратты немесе оны пайдалана алатын немесе сататын адамдарға төлем ақпаратын жібереді. Трояндардың көмегімен киберқылмыскерлер компьютеріңізді зомбиге айналдырып, оны бүкіл әлемде кибершабуылдар жасау үшін қолдана алады.

Қаскүнем электрондық почта арқылы мыналарды қамтитын (салым) хат жіберуі мүмкін:

– Антивирусты «жаңарту»

– Ақшалай ұтысқа кілт

– Қызметкерге компромат

– Апгрейд қандай да бір программа үшін (апгрейт –)

– Эротикалық мазмұндағы скрин–сейвер (скрин–сейвер –)

– Адамды жаңылыстыратын жаңалық және т.с.с..

Нәтижесінде сол хаттар салымдан файлды жүктеген кезде онлағы зиянкес программа компьютерді жұқтырады. Бұл құрбанның компьютерінде белгілі бір командыларды орындауға немесе қандай да бір қажет бағдарламаны орнатуға мүмкіндік береді.

Көбіне экранда банкерлер пайда болады, оны екі түрлі тәсілмен жабуға болады:

– Операциялық жүйені қайта орнату

– Қаскүнемге белгілі бір сумма (ақша төлеу).

Өзіңізді трояннан қалай қорғауға болады?

Трояндар осылай аталады, себебі олар сіздің компьютеріңізде іске қосылу үшін сіздің рұқсатыңызды қажет етеді - бағдарламаны өзіңіз іске қосқан кезде немесе құжатты немесе суретті ашқан кезде, оны іске қосады. Осыған сүйене отырып, трояндардан бірінші және жақсы қорғаныс ешқашан электрондық поштаның қосымшасын ашып, бағдарламаны іске қосу емес, егер сіз «тең-теңімен» бағдарламасынан немесе веб-сайттардан жүктелген файлдардың көздеріне 100% сенімді болмасаңыз. Бірақ қазіргі өзара байланысты әлемде бұл сирек мүмкін, сондықтан сізге бірнеше нақты қауіпсіздік шараларын қолдану керек.

2.6 Кері әлеуметтік инженерия

Құрбанның өзі қаскүнемнен көмек сұрап жүгінетін ситуация құруға бағытталған шабуыл.

Олар қызметтік үш бағытта жүргізеді:

– Адамдар көмек сұрауға мәжбүр болатын ситуация құру.

– Проблемаларды шешу қызметін жарнамалайды.

– Көмек көрсетеді және әрекет етеді.

Алдымен адамды немесе адамдар тобын зерттейді. Олардың қызуғышылықтары, қажеттіліктері, қалаулары, құмарлықтары, ықпалдары. Осы арқылы программалардың жеке электрондық ықпал етудің кез келген басқа әдістері көмегімен оларға әсер ете бастайды. Бастапқыда программалар ақаусыз жұмыс істейді, бұл күдік тудырмас үшін керек. Сонан соң бірте-бірте зиянды режимге көше бастайды.

Мысалы, әлеуметтік хакерлер нақты бір компания үшін программа әзірлейді. Программаға баяу іске қосылатын вирус салынған. Үш аптадан кейін ол активтеледі, ал жүйе бұзыла бастайды. Басшылық, әрине әзірлеушілерге шығады. Хакерлер де осыны күтіп отыр емес пе, өз «мамандықтарын» жібереді және құпия ақпаратқа қол жеткізу мүмкіндігін алады. Мақсатқа жетті!

Кері Әлеуметтік инженерияның әлеуметтік инженериядан айырмашылығы:

- Жұмысы ауқымды қиын;
- Ерекше білімді талап етеді;
- Тәжірибені талап етеді;
- Үлкен аудиториямен жұмыс машығын талап етеді.

Нәтижесі керемет – құрбан еш қарсылықсых, өз еркімен хакерлерге барлық картаны ашып береді.

Қарсы тұру шаралары:

- Қызметкерлерді оқыту
- Дербес ақпаратты және құпия ақпаратты ашу қаупі туралы қызметкерлерге ескерту.
- Ақпараттың сыртқа кету жолдарын бөгеу тәсілдерін үйрету.
- Қызметтік инструкция дайындау.
- Қызметкерлер құзіреттілігін анықтау.
- Тек қолдау қызметіне қандай ақпарат бермеу керектігін түсіндіру.
- Қызметкерлердің бір-бірінен ақпарат алу, ақпарат беру процедурасын анықтау.

Қызметкерлерге мынадай тыйым салынады:

- Қолданушыны тіркеу деректері компанияның меншігі болып табылады.
- Қызметкерлер компания немесе мекеме берген логин, парольдерді басқа мақсатта қолданбау туралы керек (web-сайттардан, жеке почтасында және т.с.с.),
- Логин-парольдерін үшінші жаққа немесе компанияның басқа қызметкерлеріне бермеу керек. (мысалы, отпускага кеткенде)
- Білімін, машығын жетілдіріп отыру, оқыту.
- Қауіпсіздік регламентінің болуы, сонымен қатар нұсқаулық болу керек.
- Қызметкерлердің компьютерінде өзекті антивирустық бағдарлама үнемі орнатылып тұру керек (сонымен қатар брандмауэр орнатылу керек)
- Компанияның корпоративті желісінде шабуылдарды анықтау және болдырмау жүйесін қолдану.
- Келушілермен өздерін қалай ұстау керек, ереже әзірлеу керек. Таныс емес адам көрсе, сыпайы түрде амандасып, не үшін жүргенін сұрау керек. Күдік болған жағдайда қауіпсіздік қызметіне хабарласуы керек.
- Жүйеде қолдаунушы құқығын максимальді шектеу керек. Мысалы, web-сайттарға қатысты шектеу; тасымалдауыштар қолдануға тыйым салу.

Ең бастысы: Қызметкерлерді оқыту, үйрету.

Форумның ажалы

Форум жетістігінің негізгі кепілі

- бұл оны жүргізудің сауатты саясаты және сауатты модерациялау. Осы жағдайда ғана форум - маркентингтік плюс болып табылады, қарсы жағдайда минус болмақ.

Модерациялау (модерирование) - түрлі форумдардағы, чаттардағы қолданушылардың іс-әрекеттерін (мінез-құлқы) поведение), олардың өз

хабарламаларында орналастыратын ақпараттарын бақылау, (форум ережесіне сәйкес), тексеру.

Форумды жүргізу ережелері.

- провокаторлармен, “ауани террористермен” ешқандай жағдайда сөйлеспеу (байланыспау); оларды жойып отыру (модерациялау);

- мүмкіндігінше модератор форумның қатысушысы болмағаны дұрыс. Ол оның принципиалдылығын сақтау үшін керек.

- модератор ақылды, сабырлы, тәуелсіз болуы керек. /*өзіне ұнамағанды, өзін балағаттағандарды түгел жойып отырған да дұрыс емес/.

- модератор әрекеті талқыланбайды, ол форум ережесінде жазылуы керек.

- форумда талқыланатын сұраққа өте компотентті (құзіретті) адам міндетті түрде болу керек. Кез келген мамандандырылған форумда полемика(полемика - дискусия, дебат, спор, прения) эксперттің берген сауатты, кей жағдайда жалғыз ғана дұрыс жауабынан кейін тоқтайды.

-егер сіз мамандырылған форум ұстасаңыз онда, “өмір үшін” деген бөлімді қосудың қажеті жоқ. /*өмірге деген адамдардың көзқарасы әртүрлі өз көзқарасында растап, елмен ұрысудың қажеті жоқ/

Ал форумдағы ұрыс-керіс оны “жуындыға-помойка” айналдырады.

Модерация түрлері.

1. Толық модерация (немесе премодерация). Толық модерацияланған форумға келетін әрбір хабар сайтқа жарияланбастан бұрын модератор тексеруінен өтеді.

2. Постмодерация. Егер дискуссияға және қатысушы форумның тіркелген қолданушысы болса, онда оның хабары сайтқа бірден шығады.

Мысалы: Би-би-си: тіркелген қатысушылардың хабарламаларын алдымен тексереді. Форум ережесін бұзатын кез келген хабар жойылады. Сондықтан алдымен тіркелу керек.

Дегенмен, егер қатысушы форумға тіркеліп алып, форум ережесін бірнеше мәрте бұзатын болса, онда премодерация режиміне ауыстырады немесе тіркеуден алып тастайды.

Көпшілік форумдар постмодерацияны қолданғарды жақсы көреді, адамды көп жинау үшін.

3. Жауап модерация.

Шағым түскенде ғана комментарий тексеріледі. Егер сіз форум ережесін бұзатын комментарий көрсеңіз “пожаловаться на это сообщение” сілтемесін қолданып, модераторға білдіруіңізге болады.

Би-би-си үш модерацияны да қолданады*/

Әдетте форумдарда модерацияның қандай түрі қолданылатындағы анық көрсетіледі.

Модераторды (-ларды) форум администраторы тағайындайды.

3.Әлеуметтік инженериядан қорғану және оған қарсы қолданылатын амалдар

Әлеуметтік инженерия көздері

Әлеуметтік инженерияның ең танымал әдістерінің ішінен мыналарды бөлуге болады: бейтинг немесе балық аулау (пайдаланушы алаяқтықпен қаскүнемнің сайтына апарады, содан кейін оның компьютеріне зиянды бағдарлама орнатылады), фишинг (құпия деректерді алу үшін жалған хабарламалар жіберу) және вишинг (жеке деректерді алу үшін алдын-ала жазылған дауыстық хабарламалар жүйесін пайдалану немесе жалған антивирус компьютерге зиян келтіретін (компьютерлік вирус жұқтыру және оны бағдарламалық жасақтамамен өңдеу туралы жалған хабарламаларды пайдалану)

Әлеуметтік инженерия әдістерін қалай тануға болады

Сіз кез келген сұралмаған көмек ұсыныстарынан, әсіресе үшінші тарап сілтемелерінен басуды ұсынған ұсыныстардан сақ болуыңыз керек. Әдетте, мұндай жағдайларда біз әлеуметтік инженерия туралы айтамыз. Егер пайдаланушыдан тіркелгі деректері немесе банктік ақпарат ұсыну талап етілсе, бұл ереже неғұрлым маңызды болып табылады. Бұл жағдайда алаяқтық туралы күмән жоқ, өйткені сенімді қаржы институттары ешқандай жағдайда электрондық пошта арқылы тіркелгі деректерін сұрамайды. Сонымен қатар, күдіктінің электрондық пошта хабарының жіберуші мекенжайын тексеруді ұсынамыз.

Өзіңізді әлеуметтік инженериядан қалай қорғауға болады

Әлеуметтік инженерияны физикалық тұрғыдан жою мүмкін емес. Әлеуметтік инженерияның құрбаны болмаудың ең тиімді әдісі - қырағылықты жоғалтпау және шабуылдаушылардың айласын асырып кетпеуге жол бермеу. Әлеуметтік инженерия әдістерін өз саласының кәсіпқойлары әзірлегендіктен, кейде сарапшылар алаяқтықты да тани алмайды. Сондықтан қорғаудың ең тиімді әдісі - зиянды бағдарламалардың барлық түрлерін танып, алып тастайтын заманауи антивирустық шешімді, сонымен қатар бұзылмайтын парольдерді құруға және олардың қауіпсіздігін сақтауға көмектесетін сенімді пароль менеджерін қолдануға кеңес беремін.

Қалай әлеуметтік инжинирингтің құрбанына айналмауға болады:

Егер сіз олардың дұрыстығына толық сенімді болмасаңыз, әрекет жасамаңыз.

Көмек туралы сұралмаған ұсыныстарға жауап бермеңіз

Күмәнді ақпарат көздерінің күмәнді сілтемелеріне кірмеңіз.

Жеке және банктік мәліметтеріңізді ешкіммен бөліспеңіз.

Барлық ірі компаниялар әлеуметтік инженерияны қолдана отырып, жүйеге ену сынақтарын үнемі өткізіп тұрады. Қызметкерлердің әрекеттері әдетте қасақана емес, бірақ ақпараттық қауіпсіздік үшін өте қауіпті. Сіз өзіңізді сырттан төнетін қауіптен оңай қорғай аласыз, ал іштен шыққан қауіптерден қорғану қиындыққа түседі.

Қауіпсіздікті арттыру үшін арнайы жаттығулар өткізіліп, білім деңгейі үнемі бақыланып отырады және, әрине, қызметкерлердің нақты жағдайдағы дайындығын анықтауға мүмкіндік беретін ішкі дивертация жүргізіледі. Әдетте, бұл қоңыраулар, icq, skype және әртүрлі мазмұндағы электрондық пошталар, байланыс қызметтері және әлеуметтік желілер.

Тестілеу ереже бұзушының кіруіне тосқауыл қойып қана қоймай, сонымен қатар қызметкерлердің заң бұзушылыққа деген реакциясын, олардың адалдығын тексеруге мүмкіндік береді.

Пайдаланушыларды әлеуметтік инженериядан қорғау үшін техникалық және антропогендік қорғаныс түрлерін қолданамыз.

3.1 Антропогендік қорғаныс

Антропогендік қорғаудың қарапайым әдістері:

Қауіпсіздік мәселелеріне халықтың назарын аудару.

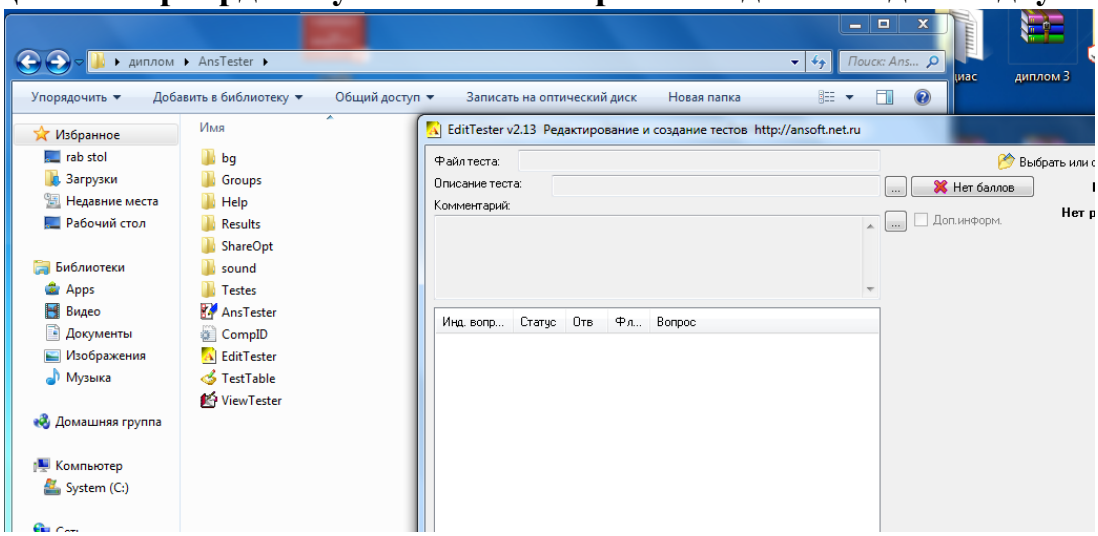
Пайдаланушылардың проблеманың ауырлығы мен жүйелік қауіпсіздік саясатын қабылдауы туралы хабардар болуы.

Ақпараттық қамтамасыз етуді қорғауды арттыру үшін қажетті әдістер мен әрекеттерді зерттеу және енгізу.

Бұлай қорғанудың бір жалпы кемшілігі бар: ол, пайдаланушылардың үлкен пайызы ескертулерге мән бермейді, тіпті ең үлкен қаріпте жазылған болсада.

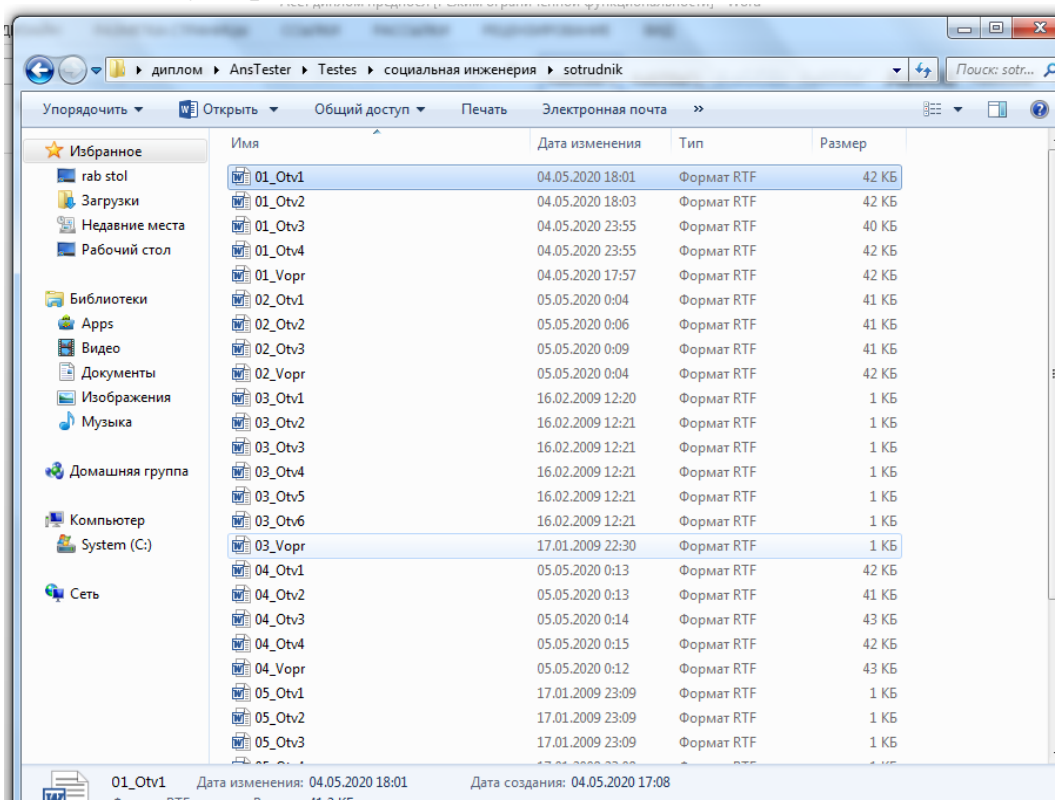
Антропогендік қорғаныстың қарапайым мысалы қызметкерлерді әлеуметтік инженерия туралы аладын-ала тесттерден өткізу

Қызметкерлерді әлеуметтік инженерияға алдын ала дайындау тесті.



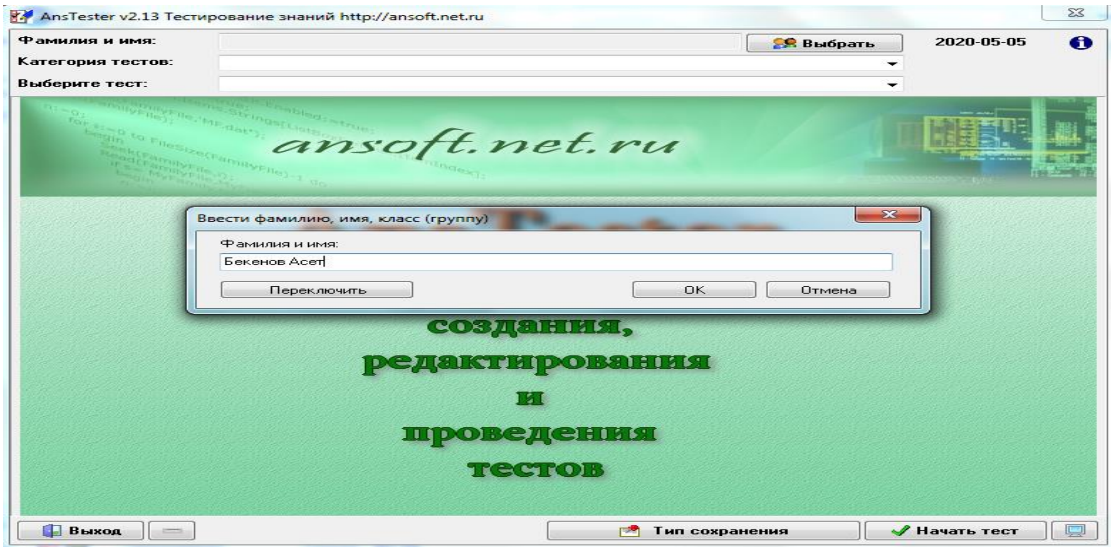
3.1- сурет. Бағдарлама интерфейсі

Тест дайындау барысы



3.2- сурет. Тест сұрақтары

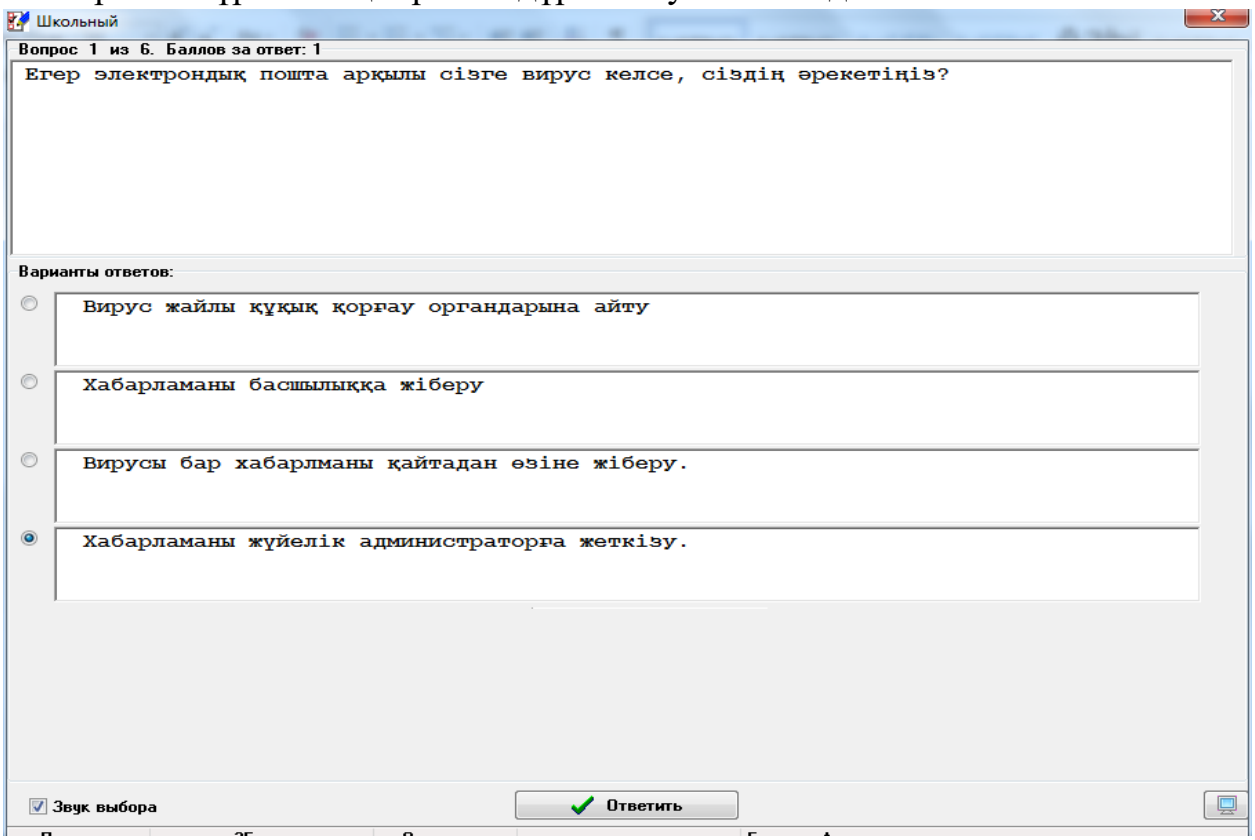
Аты-жөнімізді енгіземіз



3.3- сурет. Тест тапсыру интерфейсі

Тест бір сұраққа берілетін бірнеше жауаптардың ішінен бір ғана дұрыс жауапты таңдауға негізделген.

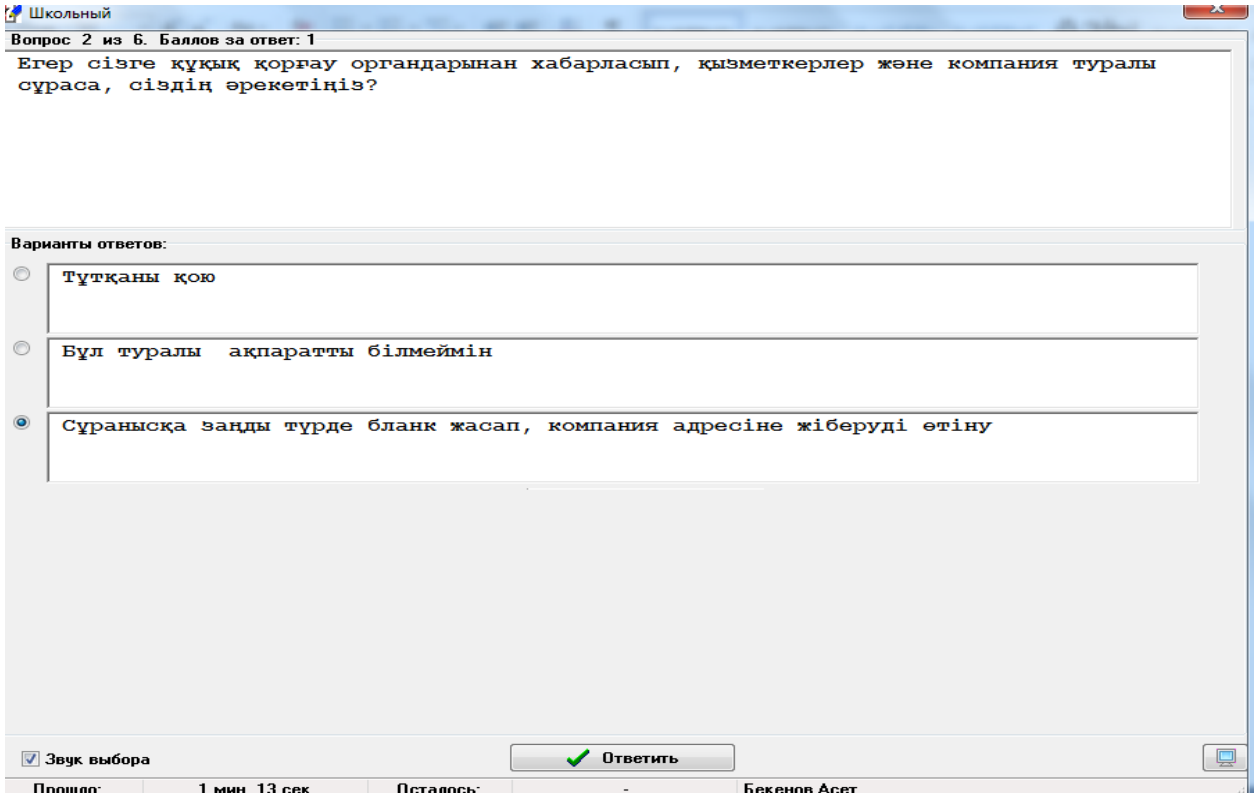
Әр тест сұрағының бір ғана дұрыс жауабы болады.



3.4- сурет. Тест сұрағы және жауаптар нұсқалары

Тест тапсырушы сұрақтарға мұқият дұрыс жауап беруі тиіс, себебі осы тест арқылы қызметкерлердің қаншалықты шабуылға дайын екенін білеміз.

Тестте жауаптар нұсқаларының саны әртүрлі болуы мүмкін. Оның санына қойылатын қатаң талап жоқ. Бірнеше дұрыс жауаптарды таңдайтын нұсқаларды әзірлеуге болады. Төмендегі суретте берілген үш жауаптан дұрысын таңдау қарастырылған.



3.5- сурет. Тест сұрағы және жауаптар нұсқалары

3.2 Техникалық қорғау

Техникалық қорғау - дегеніміз ақпаратқа қол жеткізуге кедергі келтіретін және алынған ақпаратты пайдалануға кедергі келтіретін құралдар түрі.

Адам факторының әлсіз жақтарын қолдана отырып, әлеуметтік желілердің ақпараттық кеңістігінде электронды пошталар мен ішкі желілік пошталар сияқты шабуылдар жиі кездеседі. Дәл осындай шабуылдарда техникалық қорғаудың екі әдісі де тиімді қолданылады. Кіруші хабарламалардың мәтінін (шабуыл жасаушы) және шығыс хабарламаларды (мүмкін шабуылдың нысанын) талдау арқылы кілт сөздер арқылы шабуылдаушыдан сұралған ақпаратты алуға жол бермеуге болады. Бұл әдістің кемшіліктері серверге өте үлкен жүктеме және сөздердің барлық жазылуын қамтамасыз ете алмауды қамтиды. Мысалы, шабуылдаушы бағдарламаның «пароль» сөзіне және «көрсету» сөзіне жауап беретінін білсе, шабуылдаушы оларды «парольмен» және сәйкесінше «кіру» алмастыра алады. Сәйкес таңбаларға (а, в, е, о, п, х, у, А, В, С, Е, Н, К, М, О, П, латын алфавитімен) кириллица әріптерін алмастырумен сөздерді жазу мүмкіндігін қарастырған жөн. Алынған ақпаратты пайдалануға кедергі келтіретін құралдарды мынандай түрлерге бөлуге болады:

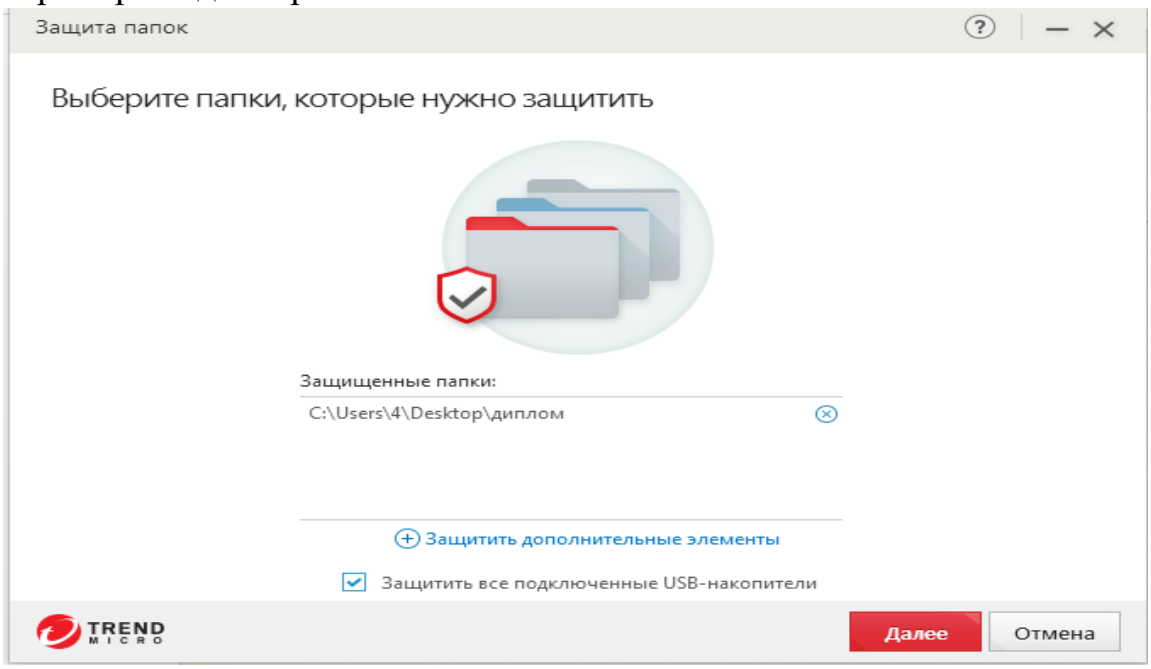
Пайдаланушының жұмыс орнынан басқа (түпнұсқалық растама деректерін сериялық нөмірлер мен компьютерлік компоненттердің электрондық қолтаңбалары, ір және физикалық мекенжайлармен байланыстыру) барлық алынған ресурстарды қолдануды бұғаттайды.

Алынған ресурстарды автоматты турде қолдануды бұғаттайды (мысалы, Captcha жүйесінің авторизациясы, пароль кезінде алдын-ала көрсетілген кескінді немесе бөлікті таңдау қажет) автоматты түрде қолдануды мүмкін етпейтін (немесе іске асыруды қиындататын) суреттер, бірақ жоғары бұрмаланған түрінде).

Бірінші және екінші жағдайда да, қажетті ақпараттың мәні мен оны алуға қажетті жұмыс арасындағы белгілі баланс пайдаланушы жағына ауысады, өйткені автоматтандыру мүмкіндігі ішінара немесе толығымен бұғатталған. Сонымен, пайдаланушының барлық мәліметтері болса да, мысалы, жарнамалық хабарламаны (спам) жаппай жіберу үшін, шабуылдаушы әр итерация кезінде жеке мәліметтерді енгізуге мәжбүр болады.

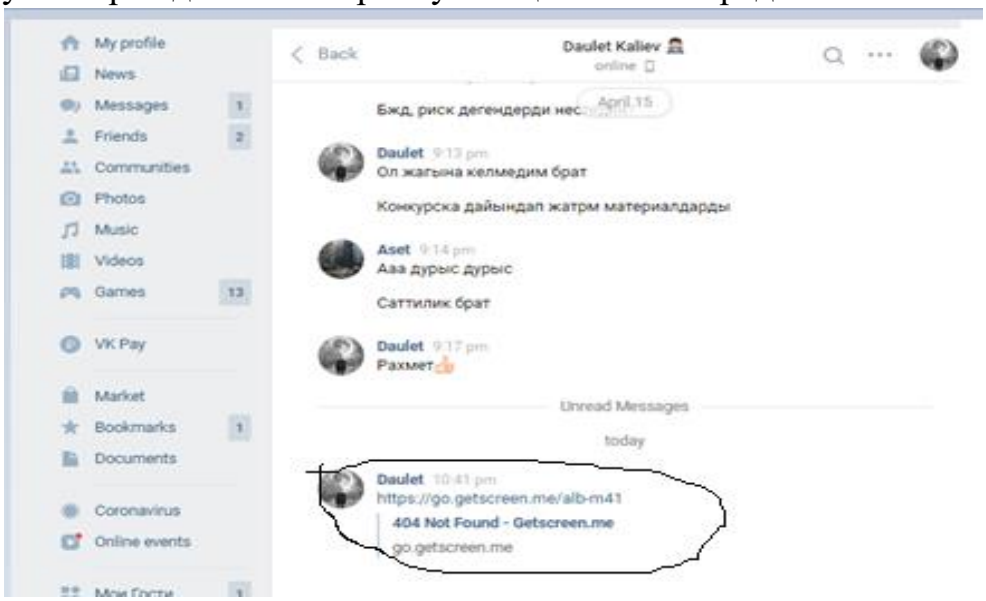
Жоғарыда атап өткендей техникалық қорғау дегеніміз ақпаратқа қол жеткізуге кедергі келтіретін және алынған ақпаратты пайдалануға кедергі келтіретін құралдар түрі.

Біз қазір бағдарлама арқылы бізге құнды ақпараттарды алдын ала қорғау шараларын ұйымдастырамыз



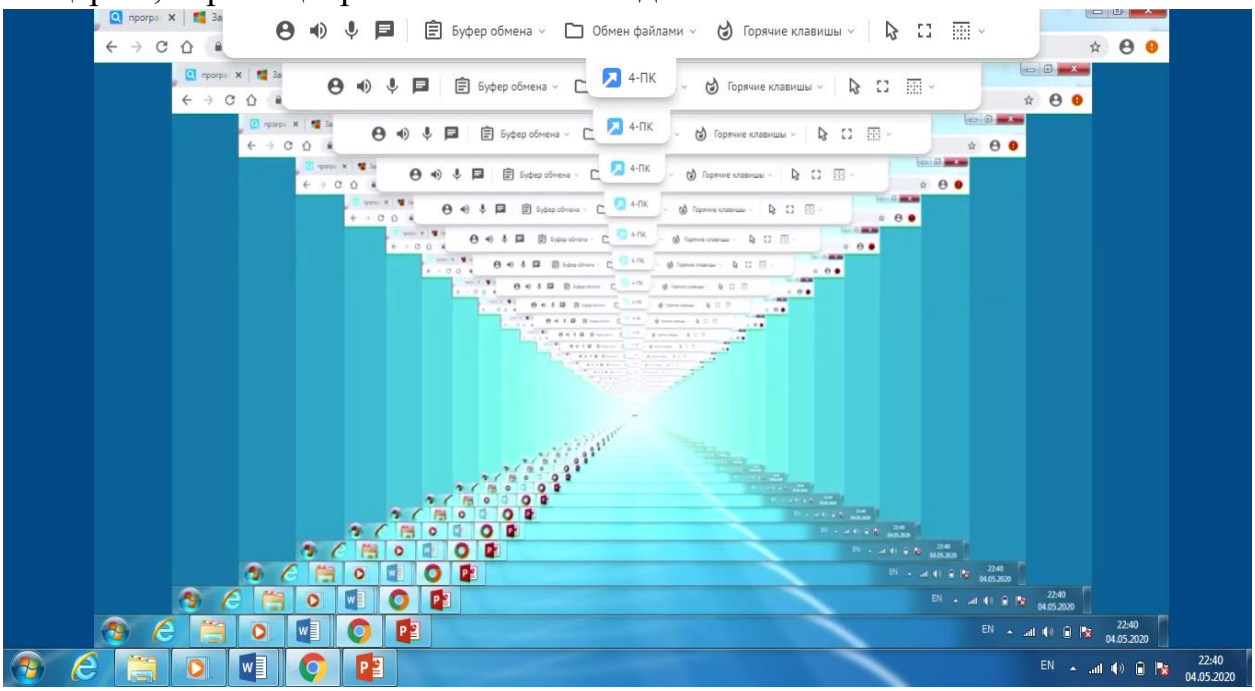
3.6- сурет. Буманы шабуылға алдын-ала дайындау

Күнделікті сөйлесіп жүрген досымыздан әлеуметтік желі арқылы бізге вирусталған ссылка келді. Біз ойланбастан сслаканы басамыз себебі шабуылдаушылар алдымен жәбірленушінің сеніміне кіреді



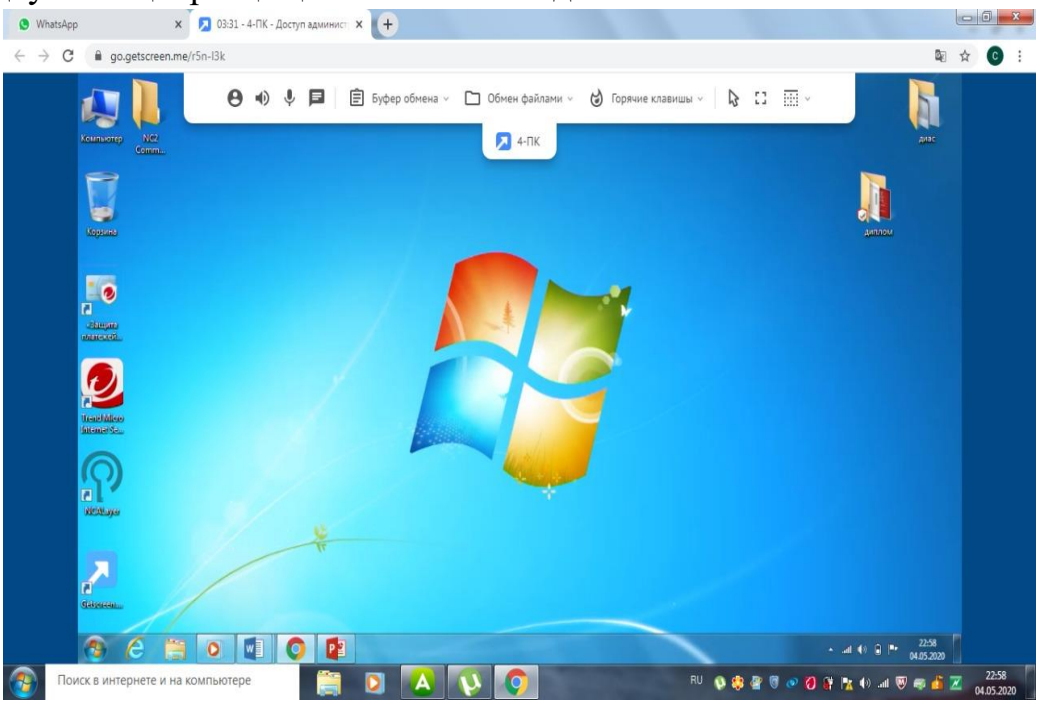
3.7- сурет. Шабуылдаушының вирусталған сслкасы.

Вирус іске қосылды. Шабуылдаушы біздің компьютермен сырттай басқарып, керек ақпаратты алғысы келеді.



3.8- сурет. Вирус іске қосылды.

Алдын-ала қорғаныс шараларын, яғни буманы қорғап қойғаннан кейін шабуылдаушы ақпаратқа қол жеткізе алмады.



3.9 – сурет. Компьютер экраны

Әлеуметтік инженерияға осалдықтың себептері

Неліктен адам ақпараттық қауіпсіздіктің әлсіз буыны болып саналады? Нақты жауап жоқ, бірақ осы тақырып бойынша сарапшылардың айтуы бойынша көптеген адамдарда пайда болатын эмоциялар қорқыныш, сенім, ашкөздік және көмектесу ниеттері осалдықтың себептері болып табылады.

Психология профессоры Роберт Циалдини өзінің «Еңсеру психологиясы» (1984) кітабында әлеуметтік инженерлер қолданатын әсер етудің алты қағидасын сипаттады:

Ынтымақтастық: біз жақсылық үшін жақсылық жасағанды жөн көреміз

Жүйелілік: біздің құндылықтарымызға сәйкес келетін сенімдерді ұстану

Әлеуметтік дәлел: көптің не істегеніне сенеміз.

Билік және абырой: біз сенетін және құрметтейтін адамдарға еруге дайынбыз

Симпатия: біз ұнайтын адамдардың өтініштерін орындауға қуаныштымыз

Жетіспеушілік: бізге қол жетпейтін нәрсені тілеу

Қызметкерлерді әлеуметтік инженерия шабуылдарынан қорғаудың тағы бір жолы ену тесті болып табылады.

Ақпараттық қауіпсіздікке соққы жасамас бұрын киберқылмыскерлердің ашылуына ену тесті көмектеседі. Бұл қызметкерлердің мінез-құлқы, компанияны қалай осал ететінін тексеруге мүмкіндік беретін жоспарланған шабуыл. Пентесталар классикалық IT ортасында да, басқа да маңызды салаларда: энергетика, көлік және ресурстарды өндіруде өткізіледі. Тест нәтижелері компания қызметкерлерінің ақпараттық қауіпсіздік қағидаларын ұстанатындығын немесе сақтамайтынын және осы мәселе бойынша олардың хабардарлығын арттыру шаралары қаншалықты тиімді екенін көрсетеді.

Кез келген салада тесттің мынадай мақсаттары болады:

Шабуыл нәтижесінде қандай ақпаратты алуға болатындығын біліңіз

Компания қызметкерлерінің психологиялық айла-шарғыға қаншалықты көнетінін анықтаңыз

Қолданыстағы ақпараттық қауіпсіздік саясатының тиімділігін бағалаңыз

Қызметкерлердің хабардарлығын арттыру бойынша шаралар кешенін әзірлеу

Кез келген ену сынағы нақты шабуылды модельдейді. Оның міндеті - компаниядағы ақпараттық қауіпсіздіктің нақты деңгейін бағалау және кибер алаяқтардан қорғау жоспарын жасау.

Пентест сәтті болу үшін, ықтимал құрбандардың нақты себептері мен қажеттіліктерін ескеріп, тестті ресми түрде жүргізбеу керек. Адаммен жасалатын қарапайым нәрсе - бұл жеке хабарламалармен қызығушылықты ояту немесе тез ақша табу мүмкіндігі, қорқыту (ол өзінің қабілетсіздігін жасырғысы келеді немесе өзін ренжіту, жазалау қаупін сезінеді), аяушылық сезімін ояту.

3.2.1 Әлеуметтік инжнериядан қорғану амалдары

Әлеуметтік инженерлік техникадан қорғану қиын, өйткені жәбірленушілер көбінесе өздерінің алданып қалғанын білмейді өздерінің әлсіз жақтарын көрсетіп қояды. Мәселені шешудің бір жолы бар: қызметкерлердің хабардарлығын арттыру. Бұл үшін оларға ақпаратпен жұмыс істеу ережелерін үйрету керек және оны жария етудің қауіптілігі туралы айту керек.

Шабуылға осал ақпаратты анықтаңыз

Қызметкерлер ақпаратты қауіпсіздік деңгейіне қарай жіктей білуі керек және қандай ақпарат компанияға зиянын тигізуі мүмкін екенін ашуды түсінуі керек. Мысалы, пайдаланушының тіркелгі деректері әрқашан ұйымға тиесілі, оларды үшінші тараппен бөлісуге немесе ашық қалдыруға болмайды. Бұл дегеніміз, логиндер / парольдер жазылған стикерлермен қоштасу керек, ашық Wi-Fi желілері арқылы корпоративтік ресурстарға кірмеу керек. Сіз болмаған кезде компьютерді немесе ноутбукті бұғаттау әдеті де көмектеседі.

Ақпараттық қауіпсіздік құзыреттіліктерін жетілдіру

Әлеуметтік инженерия әдістері үнемі жетілдіріліп отырады, ал кибер алаяқтар адамның эмоцияларында ойнаудың жаңа тәсілдерін табуда. Сондықтан компания қызметкерлері қандай ықтимал шабуылдардың құрбанына айналуы мүмкін және осындай жағдайларда өзін қалай ұстау керектігін білуі керек. Мысалы, егер алаяқтар құпия ақпарат немесе авторизация үшін деректерді сұраса, қызметкер қайда жазып кімге қоңырау шалу керек екенін білу керек.

Ақпараттық жүйелерге кіру құқығын шектеңіз

Қызметкерлер ақпараттарды көшіруге, жүктеуге, өзгертуге тек өз міндеттерін орындау үшін ғана қол жеткізе алады. Кейбір компанияларда алынбалы құралдарды пайдалануға тыйым салған жөн.

Ақпарат алмасу бойынша нұсқаулық дайындаңыз

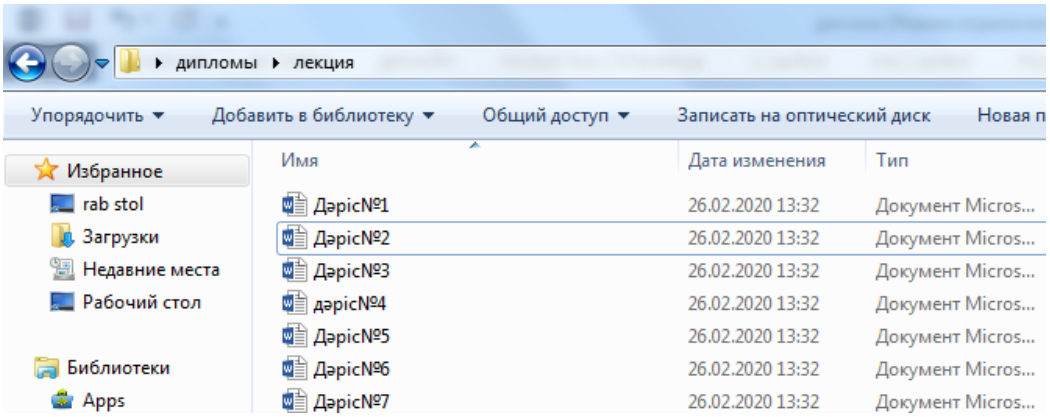
Кез-келген бөлімде және бөлімшеде қарапайым адамдардан бастап бастыққа дейін барлығы компания үшін маңызды ақпаратты аша алатын шарттар

туралы нақты нұсқауларға ие болуы керек. Нұсқаулықта техникалық қолдау қызметтеріне, реттеуші органдардың өкілдеріне және т.б. қандай ақпаратты беруге болатындығын көрсетуге болады.

Вирусқа қарсы бағдарламалық жасақтаманы соңғы нұсқаға жаңартыңыз

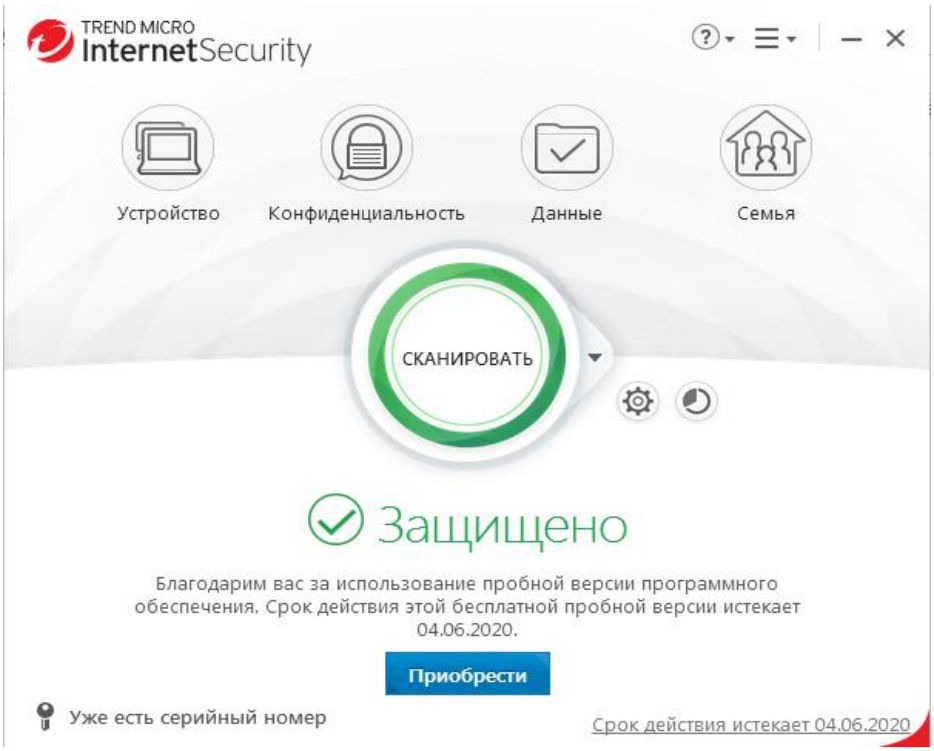
Бұл қызметкерлердің компьютерлерін жаппай фишинг шабуылдарынан әлсіз етуге көмектеседі. Қазіргі заманғы антивирустық бағдарламалар шпиондық бағдарламалар мен зиянды бағдарламалардан қорғайтын құралдарды қамтиды және күдікті сілтемелерді басқанда ескертеді. Дегенмен, жұмыс орнында әлеуметтік желілерге рұқсат бермеңіз, себебі алаяқтар әлеуметтік желілерді дегеніне жету үшін жақсы пайдаланады.

Әлеуметтік инжериядан қорғау бойынша әдістемелік тұрғыдан қамтылған қадамдары анық көрсетілген 7 дәріс жасалынды



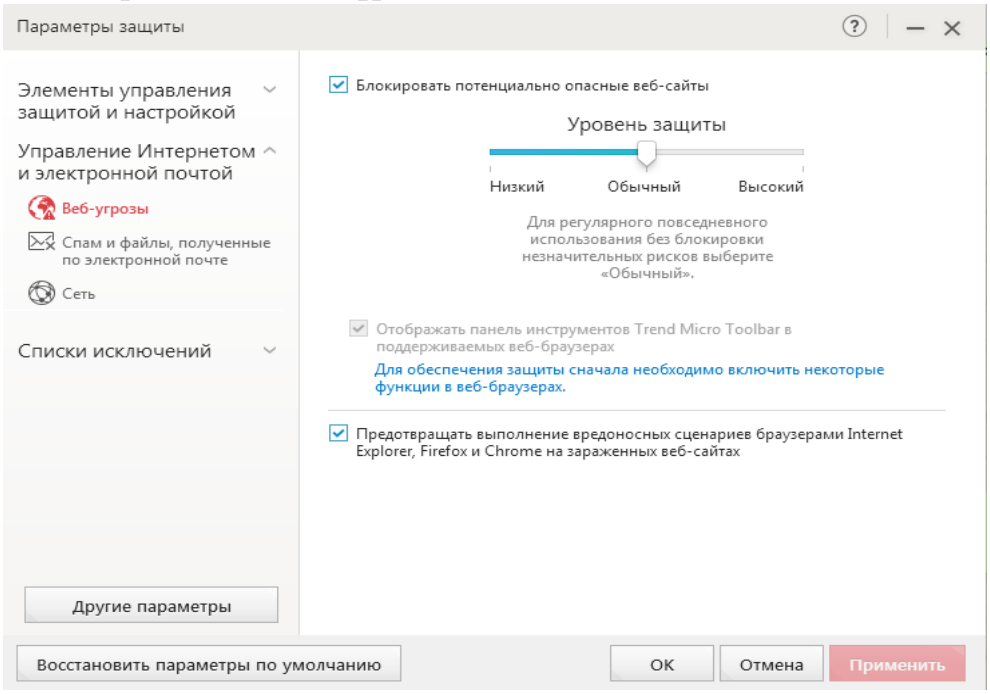
3.10- сурет. Дәрістер жинағы

Әлеуметтік инженерия, яғни фишингқа қарсы антивирустық бағдарлама



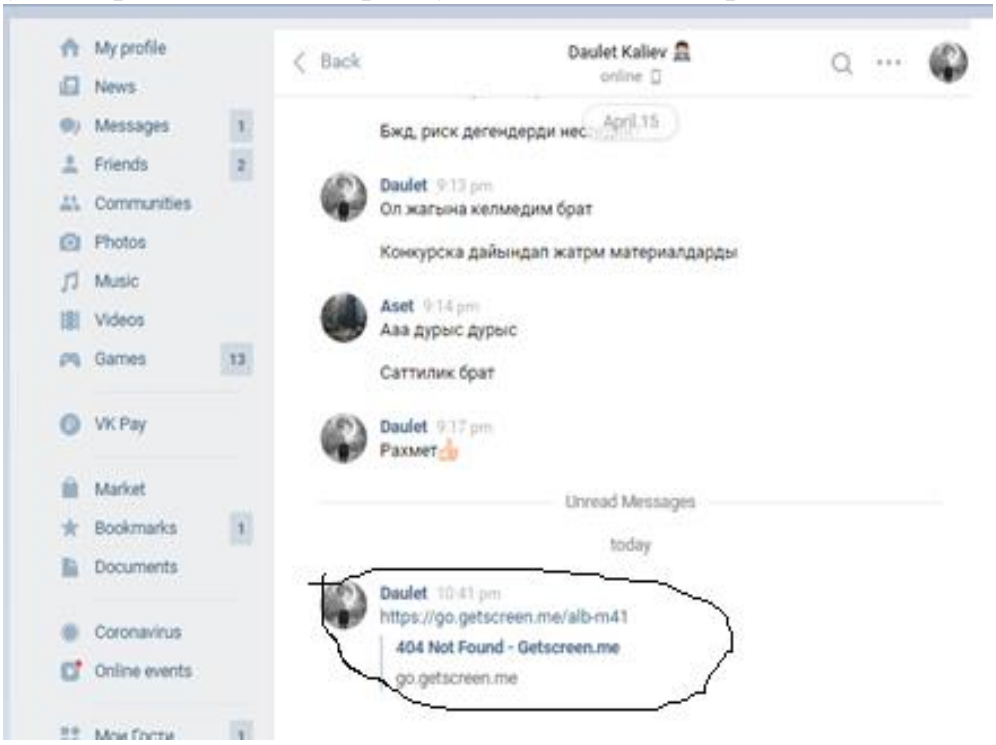
3.11- сурет. Бағдарлама интерфейсі.

Бағдарламаның баптаулары. Бұл жерде қорғаныстың деңгейін береміз, біздің жағдайда орташа болып тұр



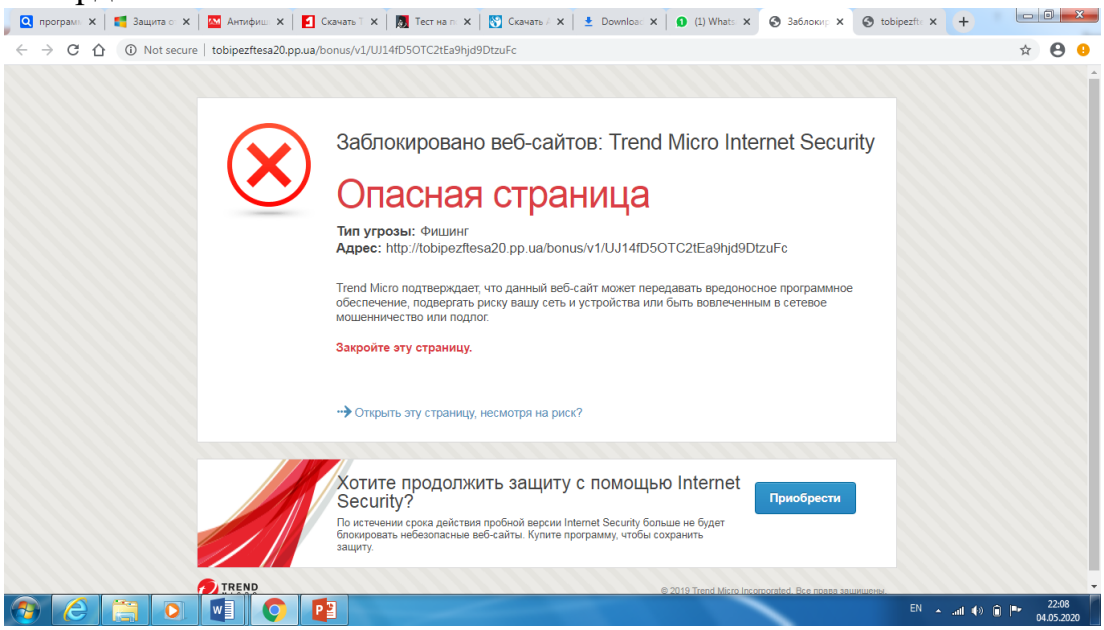
3.12- сурет. Бағдарлама интерфейсі.

Күнделікті сөйлесіп жүрген досымыздан әлеуметтік желі арқылы бізге вирусталған ссылка келді. Біз ойланбастан сслаканы басамыз себебі шабуылдаушылар алдымен жәбірленушінің сеніміне кіреді.



3.13 – сурет. Шабуылдаушыдан келген хат.

Бағдарлама күдікті сайтты бұғаттады және қандай қауіп түрі екенін анықтап берді.



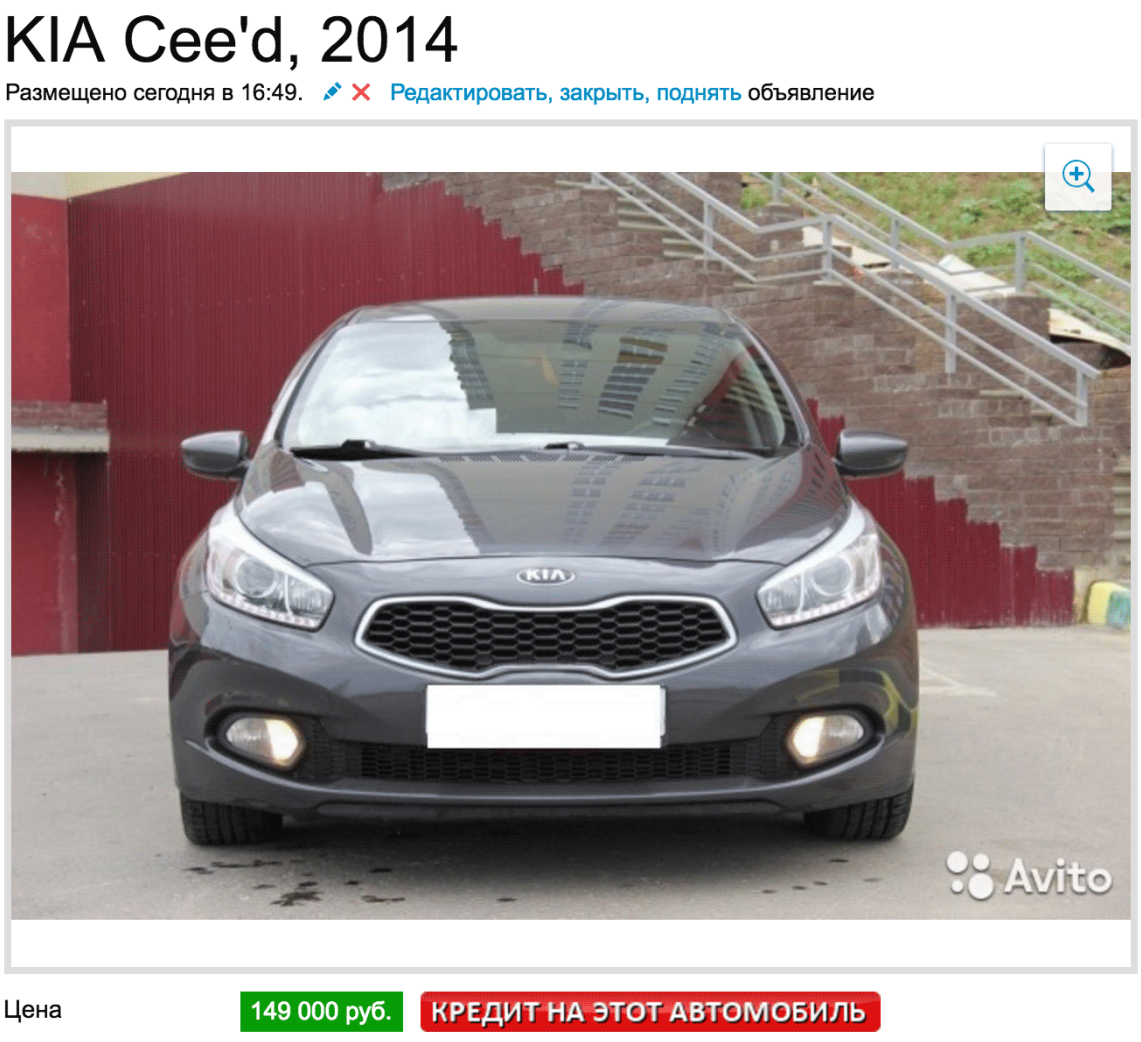
3.14- сурет. Бұғатталған парақша.

Қорытынды, қанша жерден жақын араласқан адам болсада біздер әр сслканы басарда, әр сайтқа кірерде мұқият болуымыз керек, себебі кез келген уақытта әлеуметтік инженерияның құрбаны болуымыз мүмкін.

Көптеген зерттеушілер Әлеуметтік инженерияны XXI ғ. хакерлерінің негізгі құралы санайды, неге?, себебі, техникалық қорғау құралдары күннен күнге дамуда, ал адамның әлсіз жақтары, ойламдары, стереотиптері өзгермейді. Ең керемет деген қорғау жабдығын қолданғанның өзінде де абай болуымыз керек.

3.3 Әлеуметтік желіде алаяқтардан сақтану.

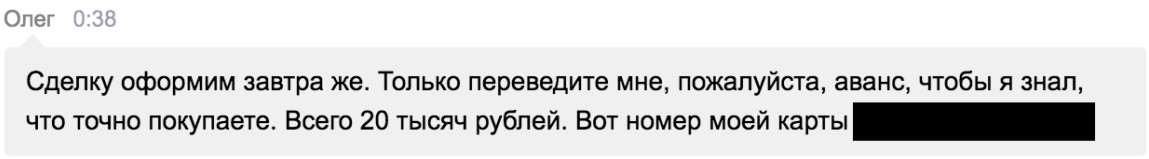
Сіз жақын арада автокөлік алуға бел будыңыз. Avito сайтына кірсеңіз онда kia ceed маркалы көлік 149000 рубль тұр, бағасы өте арзан.



3.15 – сурет. Желідегі хабрландыру.

Бағасына назар аударыңыз, бұндай автокөлік 149000 рубль тұруы мүмкін емес.

Көлік иесіне хабарласамыз, ол адам барлығын растайды, бірақ мұнда бір шикілік бар көлік иесі басқа адаммен келісіп қойған, алайда қазір алдын-ала төлемақы жіберсе көліті бізге сататынын айтады.

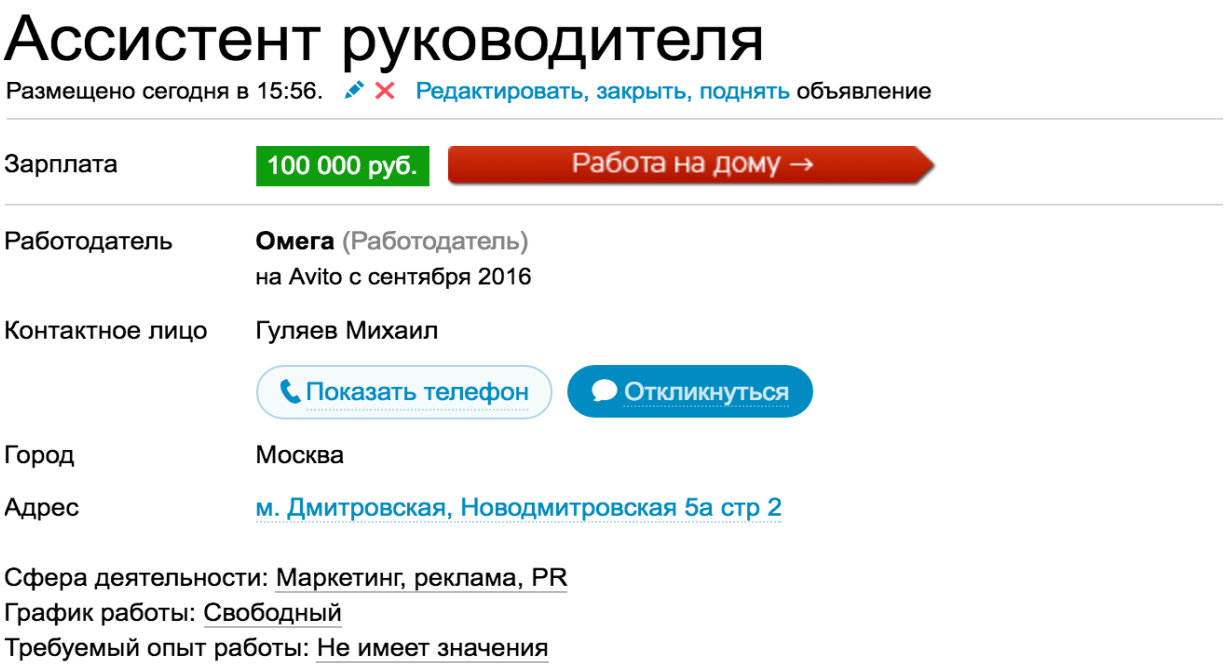


3.16 – сурет. Алаяқтан келген хат.

Егер сіз ақшаны аударып жіберсеңіз сіз алдандыңыз, сізде машина да жоқ, ақшада жок болып қалады.

Дәл осы жағдайға байланысты тағы бір мысал, Алаяқ-сатушы сізден алдын-ала өзінің жұмысы немесе товары үшін төлемақы сұрайды, ал сатып алушыны товардың арзандығы қызықтырады.

Төлемақы жайлы схеманы тек товар сатуда ғана емес, әртүрлі салада қолданады



3.17 – сурет. Желідегі хабарландыру.

Жұмысберушімен хабарласқанда, мынадай талаптары белгілі болды:

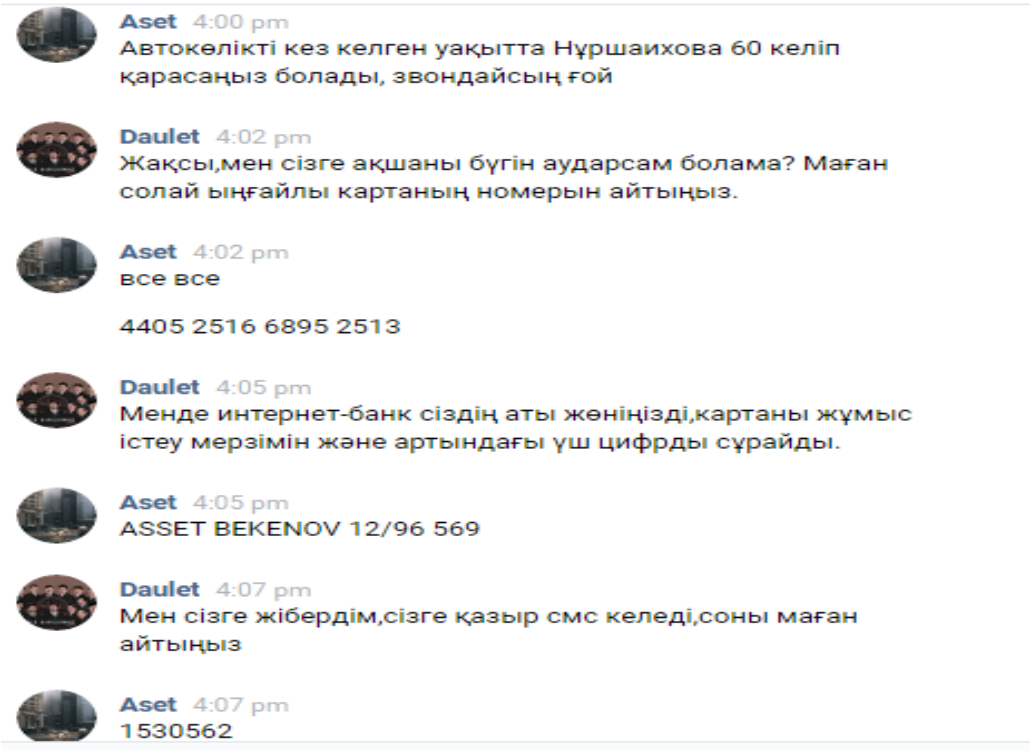
1) Жұмыс тәжірбиесі , еңбек өтілі маңызды емес

2) Ең алдымен жұмысқа кіру үшін оқыту материалдарына және сақтандыруға төлемақы жіберуіңіз керек

Егер сіз төлемақы жіберсеңіз жұмысберушіні осыдан кейін көрмейсіз. Көп жағдайда жұмысберуші, жұмыс тәжірбиесі мен еңбек өтілін талап етеді. Сондықтан төлемақы жіберуге асықпаңыз.

«Карта туралы мәліметтерді айтыңыз»

Бұл қалай жұмыс істейді, алаяқ хабарландыруға жауап береді, тауар үшін алдын-ала төлем ұсынады және сатушыдан карта деректерін сұрайды. Сонымен қатар, ол тек карта нөмірін ғана емес, сонымен қатар SMS-тен немесе артқы жағынан да код сұрайды. Осы мәліметтермен алаяқ картадағы ақшаны ұрлайды.



3.18 – сурет. Алаяқпен сойлесу барысы.

Сіз автокөлігіңізді сатып алғысы келетін сатып алушыны таптыңыз деп елестетіп көріңіз. Жас жігіт сізге хат жазады, көлік туралы сұрақтар қоймайды

және тіпті алдын ала төлем ұсынады. Ақша сізге ұсынылғандықтан, ешқандай қауіп жоқ сияқты.

Қымбат сатып алушыны жоғалтпау үшін сіз оған аударым туралы сұрайтынның барлығын айтасыз: карта нөмірі, аты, жарамдылық мерзімі, артқы жағындағы нөмірлер және SMS-тен растау коды. Ал, аударым үшін тек карта нөмірі жеткілікті.

Жалпы әлеуметтік желедігі қорғану амалдары:

- Алдын ала төлем жасауға асықпаңыз.

- Ешкімге картаның мәліметтерін айтпаңыз және sms кодтарды бермеңіз.

- Сілтемелерді орындамаңыз немесе бейтаныс адамдар жіберген файлдарды ашпаңыз.

- Ертегі ұсыныстарға сенбеңіз, сіз дүкендегіден он есе аз өнім көрсеіңіз, бұл жалған.

- Егер сіз алаяқтыққа күмәндансаңыз, «Шағымдану» түймесін басыңыз.

3.4 Әлеуметтік инженериялық тренинг

Әлеуметтік инженериялық тренинг – өзін-өзі тануға, өзін-өзі реттеуге, тұлғааралық қарым – қатынасқа түсу барысында , басқа адамдардың іс-әрекетін , жымысқы ойын жақсы түсінуге көмектеседі, өз бейнесін , тұрақтылығын басқалар қалай көретіндігін салыстыруға мүмкіндік береді, өз мүмкіндігін байқауға, өзіндік санасын жетілдіруге жағдай жасайды. Әлеуметтік инженериялық тренинг саналы жұмыс түріне баулиды: мұнда өз көзқарасын қалыптастырады,қауіп қатерді дұрыс жүйелеуге, өз білімін іс әрекетте қолдануға дағдыланады. Адамды күтпеген оқыс шабуылда ойлану мен шешім қабылдауға үйренеді.

Әлеуметтік инженериялық тренинг қалай жүргізіледі және ол не береді? Тренинг барысында адамдарға әртүрлі әдістер мен жаттығуларды орындату керек . Осындай рәсімдердің негізгі мақсаты - әлеуметтік инженериялық шабуылға қарсылық білдіруге, өз тәжірибеңізді түсінуге көмектесу және қиындықтарды тиімді шешу дағдыларына ие болу. Тренингтің бірегейлігі - әлеуметтік инженериялық шабуылға қарсылық білдіруге, мінез қалыптастыру.

Қызметкерлер қалыптасқан тұрақты мінездерінің басқаша жағынан көруге, басқа адамдардың жымысқы іс әрекетін , ойын жақсы түсінуге көмектеседі, өз бейнесін басқалар қалай көретіндігін салыстыруға мүмкіндік береді, өз мүмкіндігін байқауға, өзіндік санасын жетілдіруге жағдай жасайды. Қызметкерлер әлеуметтік инженериялық шабуылға қарсы өздерінің мәселелерін шешудің жолы тек жетекшінің көмегіне ғана емес, сонымен қатар , басқа топтың қолдауына да ие болады. Жалпы алғанда, бұл топ «терапевтік» әсерге ие, өйткені әрбір қызметкер өзінің жеке бастамасы бойынша басқа адамның да әлеуметтік инженериялық шабуылға қарсылық білдіруге, мінез қалыптастыру мәселесіне бірегей жауап бере алады және әр түрлі көзқарастарды ескере отырып түсінуге мүмкіндік береді. Сіздердің назарларыңызға әлеуметтік инженериялық шабуылға қарсылық білдіруге, мінез қалыптастыруға бағытталған бірнеше ойын жаттығуларын ұсынғым келеді.

Барысы:

Кіріспе әңгіме. Әлеуметтік инженериялық тренинг -жаттығуымызды бастаймыз. Кез-келген тренингтің өз ережелері бар. Қызметкерлердің барлығы белсенді жұмыс істеуге, ұсынылған жаттығуларға белсенді қатысуға, бір-бірін мұқият тыңдауға кеңес береге әлеуметтік инженериялық тренинг түрткі болады деп сенім бар : адамның эмоционалды жағдайына, өзімізді және басқаларды жақсы түсінуге, өз сезімдерін, тәжірибесін, реаксация әдістеріне үйренуге және уақытты жақсы өткізуге арналған. Әлеуметтік инженериялық тренинг барысында белгілі бір жолмен жүріп өтуі керек, әдеттегідей, тренинг сәлемдесу мен таныстырудан басталады.

1. «Танысу» жаттығуы. Мақсаты: Топтың мүшелеріне бір-бірімен танысуға көмектесу, топтағы эмоционалдық жағымды жағдайды қалыптастыру және қызметкерлер өзін-өзі бағалауы.(Жүргізуші жаттығуларды бірінші болып өзі орындай бастайды). Жүргізуші өз есімін айта отырып, сол есіміне сәйкес бірінші әріптен басталуы шарт өзінің бойындағы жақсы қасиетін ескеріп жаңа есіммен атайды, мысалы: Сезім - «нәзік». Келесі қатысушы өзінің есімі мен бойындағы жақсы қасиетті қосып атайды және солай жалғаса береді. Бұл әлеуметтік инженериялық шабуылға қарсылық білдіруге, мінез қалыптастырады.

2. «Өзіңді мадақта» жаттығуы. Мақсаты: стресті жеңілдету, топта көңілді атмосфераны қалыптастыру.Өзімен жақсы қарым-қатынас орнатуға көмектесетін тамаша жаттығу бар. Өзімізді қаншалықты жиі мадақтаймыз? Әдетте, біздің басымыз теріс баптауларға толы: «Осы жерде басқаша жасауым керек еді...», «Мұнда жеткілікті жақсы жұмыс атқара алмадым...», немесе, «Адамдардың

айтқан ойының жетегіне, көзімді жеткізбей тұрып, ілесіп кете беремін .... ». Осы ойлардың көпшілігін өзіміз байқамаймыз. Біз үнемі өзімізді сынауға әдеттенгенбіз. Мұндай ойларымызды тез арада өзгерту өте маңызды! Қатысушыларға өз бойындағы өздеріне ұнайтын немесе басқалардан ерекшеленетін қасиеттері туралы ойлануға және айтуға шақырылады. Бұл кейіпкер мен тұлғаның кез-келген жақсы ерекшелігі болуы мүмкін. Бұл да әлеуметтік инженериялық шабуылға қарсылық білдіруге, сенім тудыратын мінез қалыптастырады.Тағыда басқа тренингтарды жүргізуге болады

Естеріңізге салайлық, бойыңыздағы бұл жақсы қасиеттер, сізді ерекшелендіреді.

Сонымен қоса , қызметкерлер арасында әлеуметтік инженериялық шабуылға қарсылық білдіруге Дж. Моренонын «Социометрия» әдісін қолдануда тиімді.

Дж. Моренонын «Социометрия» әдісі бойынша қызметкерлер арасындағы әлеуметтік инженериялық шабуылға қарсылық білдіруге қасиеттерінің зерттеу жұмысының нәтижелері туралы қорытынды

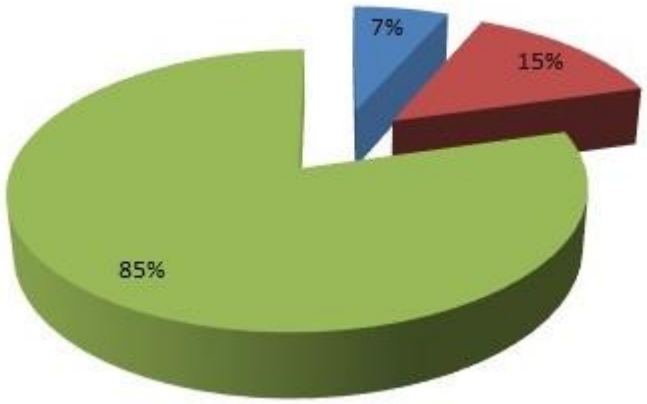
Мақсаты:

Қызметкерлер арасындағы әлеуметтік инженериялық шабуылға қарсылық білдіруге әлсіздер , дайын еместер , дайындарды анықтау

Зерттеудің нәтижесі бойынша анықталғаны:

Қызметкерлер саны	әлеуметтік инженериялық шабуылға қарсылық білдіруге әлсіздер	әлеуметтік инженериялық шабуылға қарсылық білдіруге дайын еместер	әлеуметтік инженериялық шабуылға қарсылық білдіруге дайындар	Қамтылмай қалған қызметкерлер
82	6 - 7%	12 - 15%	64 – 78 %	-

3.1 – кесте. Зерттеу нәтижесі.



Сурет -3.19. Зерттеу нәтижесінің көрсеткіштеріне құрылған диаграмма.

Қорытынды:

Қызметкерлер арасынды өткізілген «Социометрия» әдісі бойынша әлеуметтік инженериялық шабуылға қарсылық білдіруге әлсіздердің аз да болса бар екенін, дайын еместер аз мөлшерде екенін,ал , дайындар қызметкерлердің көп мөлшерде екендігі қуантады.

Бұл әдіс жанама сұрақтар қою арқылы , әлеуметтік инженериялық шабуылға қарсылық білдіруге анықтауға, қызметкерлердің әлеуметтік инженериялық шабуылға қарсылық білдіруге білімінің қаншалықты екенін білуге мүмкіндік береді. Мұндай тәсілдердің құндылығы сол, әлеуметтік инженериялық шабуылға қарсылық білдіруге мінездерінің тұрақтылығын анықтауға мүмкіндік береді.

4 Өмір-тіршілік қауіпсіздігі бөлімі

4.1 Жұмыс жағдайын талдау

Дипломдық жұмыстың бұл бөлімінде «Әлеуметтік инженерия ақпараттық қауіпсіздік аспектісінде пәні бойынша зертханалаық жұмыстар әдістемесін әзірлеу» бағдарламашы-әзірлеушінің жұмыс орнын ұйымдастырудың оңтайлы шарттары сипатталды, табиғи жарықтандыруды, өрт қауіпсіздігін және желдету жүйесін есептеу туралы шешім қабылданды.

Жұмыс орнында программисттерге екі ноутбук және модем орнатылған. Ноутбуктар ғаламторға Wi-fi арқылы немесе RJ-45 кабелі арқылы модемге байланысады.

Санитарлық-эпидемиологиялық нұсқауларға сәйкес қондырғы көздерімен жұмыс істеу жағдайларына қойылатын физикалық факторлар (ДК) әсер ететін адамдарға жеңіл 1б санатта қолайлы микроклиматтық көрсеткіштер мынадай шарттар болып табылады:

- қыста температура 23-21^{o}С, жылдың ыстық мезгілінде 22-24^{o}С, мұндағы ауа ылғалдылығы 40 - 60%;

- жылдың ыстық мезгілінде ауа айналымының жылдамдығы 0,2 м/с, қыста 0,1 м/с.

Бұл көрсеткіштер жұмыс орнында іске асырылуы тиіс. Барлық электроника өрттің әлеуетті көзі болып табылады. Өрт туындауының алдын алу үшін электрондық техника қауіпсіздік шаралары сақталынды: техника мен электр кабельдерінің дұрыс орналастырылды. Сондай-ақ инциденттердің туындауын болдырмау үшін физикалық әсерден қорғалған электр желісі, электрмен қоректендіруге қосудың сапалы нүктелерін, өрт қауіпсіздігі шараларын қатаң сақтауды, электр желісіне жүктемені сауатты есептеуді, жабдықты шаңмен немесе басқа заттармен ластанудан тұрақты тазалау жүзеге асырылды, электр қоректендіруге қосу нүктелерінде тұйықталуды болдырмау үшін физикалық әсер мөлшерін азайтылды. Электротехниканың жұмысы барысында электр өрісі пайда болады, ол әртүрлі жақын тұрған заттарға әсер етеді. Мысалы, компьютер кулерінің жұмысы кезінде электрлендірілген шаңның шығуы орын алады, ол адамға кері әсер етеді. Компьютерлік мониторлар статикалық электрдің күшті жинақтаушысы болып табылады. Бүгінгі таңда адамға статикалық электрдің қандай әсер ететіні туралы толыққанды деректер жоқ. Зерттеулерге сәйкес, статикалық электрдің әсерінен адамның терісінің жүйке бітеулерінің тітіркенуі болады, сондай-ақ бұл әсер матаның иондық құрамының өзгеруін тудырады.

Бұл әсерлердің барлығы шаршауға, толыққанды болмаған ұйқыға және тітіркенуге әкеледі. Статикалық электрдің адамға кері әсерін болдырмау үшін ұсыныстар мынадай: жұмыс кеңістігі шегінде ауаны ылғалдандыру, ылғалды жинау (ылғалдылығы 50% - дан артық емес), электротехниканы жерге тұйықтау,

бөлмені тұрақты желдетілуін ұйымдастыру. Сонымен қатар ДК-мен ұзақ жұмыс кезінде адамға электромагниттік әсердің пайда болуы ықтималдығы үлкен. Бұл әсерді болдырмау үшін бөлмені тұрақты желдету, физикалық жүктеме, жұмыс орнына тек барлық қауіпсіздік шаралары мен санитарлық нормаларға жауап беретін ғана сапалы жабдықты орнату ұсынылады.

Компьютермен жұмыс істеу кезінде маңызды аспектілердің бірі бөлменің жарықтандырылуы болып саналады. Табиғи жарықтандыру өте маңызды, сондықтан компьютердің терезеге қатысты орналасуы өте маңызды. Компьютерді терезеден жарық тікелей түспейтіндей орналастырылды. Әйтпесе, бұл жұмыс кезінде көздің шаршауына себеп болады. Шешім - күн сәулесінен қорғайтын жалюзи немесе тығыз перделерді қолдану.

Жұмыс кезінде компьютерді пайдаланушыға әсер ететін жоғарыда айтылған зиянды және қауіпті жағдайлардан басқа, компьютерде жұмысты дұрыс ұйымдастырмаудан туындаған басқа да зиянды жағдайларды да бөліп көрсетілді. Осылайша, ұзақ отырып жұмыс істеу адамға зиян болып саналады, жұмыс орнын ұйымдастыруға көп көңіл бөлінді. Ұзақ уақыт бойы бір қалыпта болуы бұлшықетті үнемі демалыссыз жұмыс істеуге мәжбүр етеді. Аз қозғалу - компьютерлерді пайдаланушылардың және бағдарламалық қамтамасыз етуді әзірлеушілердің басты проблемасы. Ұзақ отырудан туындаған физиологиялық қызметтің азаюы кезінде семіздік, геморрой, остеохондроз сияқты ауру қаупі артады. Дұрыс емес қалыпта отырғандағы бүкірлік арқылы дискілерді деформациялап, жарақаттап, омыртқаға теріс әсер етеді.

Бұрын сипатталған психофизиологиялық қауіпті және зиянды жағдайлар әсер ету сипаты бойынша мынадай бөлінеді:

- физикалық (статикалық және динамикалық);

- жүйке-психикалық (ақыл-ойдың артық тырысуы, талдағыштардың артық тырысуы, еңбектің монотондылығы және эмоциялық артық жүктеме).

Компьютерде жұмысты ұйымдастыру шарттары:

- жұмыс бөлмесінде табиғи және жасанды жарықтандырудың болуы;

- бөлмені кондиционерлеу жүйелерімен немесе тиімді желдеткішпен жабдықталуы; бөлме сағат сайын желдетіледі;

- бөлменің күнделікті ылғалды тазалау;

- күн сәулесінің тікелей түсуінен аулақ болу үшін перделерден немесе жалюздерден пайдалану;

- біркелкі жасанды жарықтандыру. Барлық еңбек нормаларын сақтау үшін қажет қосалқы есептеулер бұдан әрі келтірілген

4.1.1 Жұмыс орнының сипаттамасы

Ғимаратты жобалау және құру кезіндегі мәліметтерді әдістемілік нұсқаудан алынды [1].

Жұмыс орны - бұл орындық, үстел, компьютер орналасқан бөлме (5.1-сурет, бөлменің өлшемдері миллиметрмен көрсетілген).

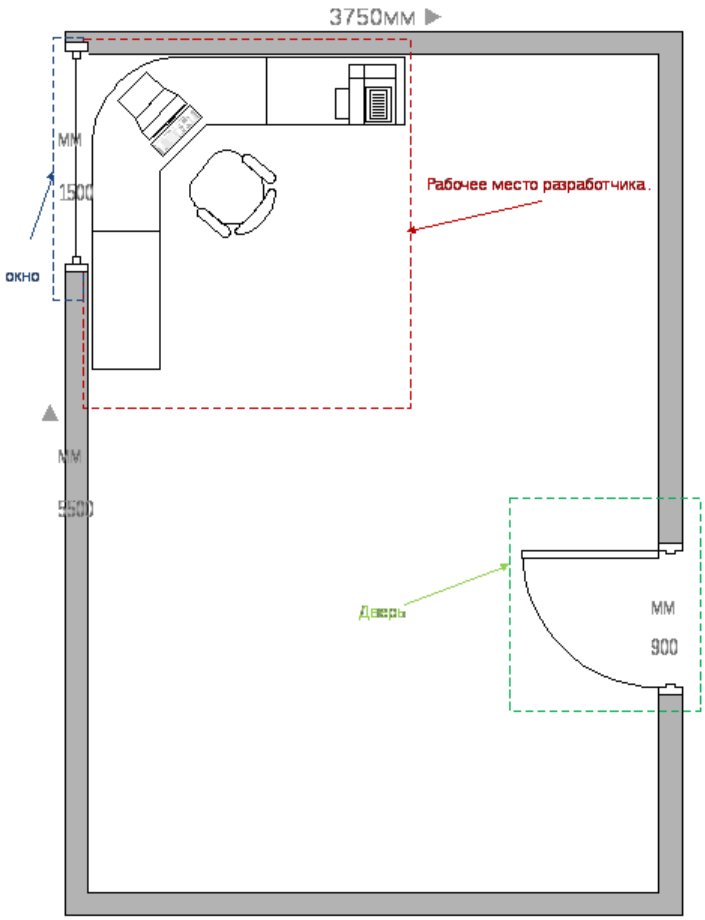
Бөлмеде келесі параметрлер бар:

− бөлме өлшемдері: ұзындығы 5.5 м, ені 3.75 м, биіктігі 2.8 м;

− жарық өткізгіш материалдың түрі − шыны парағы, қос; − байланыстың түрі − болат, қосарлы, ашылады;

− терезенің өлшемі 1,5 м*1,2 м;

− есіктің өлшемі 60 см*2 м;



Сурет 4.1 − Бөлме жоспары

4.1.2 Жарықтандыру жүйесі

Бөлменің жарықтандыру жүйесі жобалауы СНиП РК 2.04-05-2002 [2] 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;
- жарықтандыру пульсациясының тереңдігі шектеледі.

4.1.3 Желдету жүйесі

Мәліметтер әдістемелік нұсқаудан [3] алынды.

Желдетуді жобалау кезінде, ең алдымен, өндірістік бөлмені және ондағы технологиялық процестерді сипаттау қажет. Менің жобамда бөлме - бұл ақпараттық жүйені бағдарламашы-әзірлеуші жұмыс істейтін кеңсенің бір бөлігінде жасалған бөлме. Бөлмеде оның қасында жиһаз бен компьютер бар.

Ауаны шығаратын желдету қондырғыларының өрт қауіптілігі сұйықтықтар, газдар, шаңның ыстық буын қамти отырып, жарылысы қауіпті бу, газ, шаң-ауа қоспасының түзілу мүмкіндігіне байланысты. Ыстық шаңның маңызды мөлшері ауа арнасында және тазарту қондырғыларында жинақталуы мүмкін. Жүйені тоқтағаннан және оның соңғы рет қосқаннан кейін шөккен шаң өлшенген күйге көше алады және осылайша жарылуы қауіпті шаң-ауа қоспасын түзеді.

Мұндай қоспалардың тұтану көздері мыналар :

- өндірістік жабдықтардағы ұшқын мен тұтану;
- желдеткіш ротор қалағымен соғылғанда шығатын ұшқын;
- жатып қалған шаңның өздігінен тұтануы;
- желдету камераларында орнатылған электр қозғалтқыштарды аса қыздыру;
- статикалық электр.

Ауамен жылыту жүйесінің ауа таратқышынан шығатын ауа температурасы 60°С-тан артық емес, бірақ жайда бөлінетін газ, бу, аэрозоль мен шаңның өздігінен тұтану температурасынан 20 %-дай кем. Ауа температурасы сыртқы есіктерде 50°С-тан жоғары емес, ауа пердесінен ауаны шығару кезінде сыртқы қақпа мен технологиялық ойықтарда 70°С болады.

Жергілікті сору жүйесімен шығарылған ауада ыстық газ, бу, аэрозоль мен шаңның шоғырлануы атмосфералық қысым және шығарылатын қоспа температура кезінде жалын таралуының төменгі шоғырланған шегі 50 %-дан аспайды.

А және **Б** категориядағы жайларды апатты желдетуді орнатады және жасанды қозғағышы болуы және соратыны болады. Ауаға ыстық газ бен буды шығару оңай болатын бір қабатты ғимараттарда ағынды апатты желдетуді орнатады. Ауа шығыны туралы технологиялық деректер болмағанда биіктігі 6 м-ге дейінгі жайда жай еденінің 1 $м^2$ ауданынан 50 $м^3/с$ кем емес 8 еселік апатты ауа алмасу қабылданады. **А** және **Б** категориялы сорғы және компрессорлық станцияларда жоғарыда көрсетілген ауа алмасу негізгі жүйені қамтамасыз ететін ауа алмасуға қосымша жобаланады.

Апатты желдету үшін жеткілікті ауа шығынын қамтамасыз ететін соратын желдетудің негізгі жүйесі пайдаланылады. Негізгі жүйелерде резервті желдеткіштер болмағанда тек ауаның максимум шығыны бар жүйелері үшін ғана

резервті желдеткіш (өндірісте бір уақытта бір апатты есепке алу немесе резервтік желдеткішті орнату) жобаланады. Егер негізгі жүйенің ауа шығыны апатты желдетуі үшін жеткіліксіз болса, онда осы жүйелердің үлкеніне резервті желдеткіш орнатады және апатты желдеткішті жеткіліксіз шығын ретінде қарастырады. Апатты желдеткішке резервті желдеткіштер жобаланбайды.

4.1.4 Өрт қауіпсіздігі

Өрт қауіпсіздігі персоналдың жұмыс ортасының қауіпсіздігін қамтамасыз етудегі ҚР ҚНжЕ 2.02-05-2009 [4] .-құрылыс проект нормасымен анықталады. Өрт қауіпсіздігі-өрт мүмкіндігін толық жоққа шығаратын, ал ол туындаған жағдайда адамдарға өрттің жағымсыз факторларының әсерін болдырмайтын және жұмыс ортасы мен материалдарын қорғау қамтамасыз етілетін объектінің жай-күйі.

Өрт қауіпсіздігі өрттің алдын алу жүйесімен және өрттен қорғау жүйесімен қамтамасыз етілді.

Жұмыс орнындағы өрттер аса қауіпті, себебі үлкен материалдық шығындармен байланысты. Жұмыс орнының ерекшелігі - бөлменің шағын аудандары. Өрт жанғыш заттардың, тотығу мен тұтану көздерінің өзара әрекеттесуі кезінде туындайды. Жұмыс орнында өрт пайда болу үшін қажетті барлық үш негізгі фактор бар.

Жанғыш компоненттерге бөлмені әрлеуге арналған материалдар, қалқалар, есіктер, едендер, кабельдерді оқшаулау және т. б. жатады.

Өртке қарсы қорғаныс - бұл адамдардың қауіпсіздігін қамтамасыз етуге, өрттің алдын алуға, оның таралуын шектеуге, сондай-ақ өртті сәтті сөндіру үшін жағдай жасауға бағытталған ұйымдастырушылық және техникалық іс-шаралар кешені.

От алдыру көздері ЭЕМ-нің электрондық схемалары, техникалық қызмет көрсету үшін қолданылатын аспаптар, жануға қабілетті электрмен қоректендіру құрылғылары болып саналады. Сондай-ақ оларды ӨҚ талаптарына сәйкес келмейтін жағдайда сақтау немесе пайдалану.

Жұмыс орнындағы өрт өте қолайсыз салдары: құнды ақпараттың жоғалуы, мүліктің бүлінуі, адамдардың қаза болуы және т. б.

Өрттің шығу себептері:

- электр сымдарының, розеткалар мен ажыратқыштардың қысқа тұйықталуына немесе оқшаулау сынамасына әкелу ақаулары;
- ақаулы электр құралдарын пайдалану;
- бөлмені ашық қыздыру элементтері бар электр қыздыру аспаптарын пайдалану;
- ғимаратқа найзағайдың түсуі салдарынан;
- ғимараттың жануына ықпал ететін сыртқы әсерлер;

- отты ұқыпсыз қолдану және өрт қауіпсіздігі шараларын сақтамау.

Өрт алдын алу адамдардың қауіпсіздігін қамтамасыз етуге, өрттің алдын алуға, оның таралуын шектеуге, сондай-ақ өртті сәтті сөндіру үшін 81 жағдай жасауға бағытталған ұйымдастырушылық және техникалық іс-шаралар кешені болып табылады. Өрттің алдын алу үшін ғимараттың өрт қауіптілігін дұрыс бағалау, қауіпті факторларды анықтау және өрт алдын алу және қорғау тәсілдері мен құралдарын негіздеу өте маңызды.

Өрт қауіпсіздігін қамтамасыз ету шарттарының бірі-тұтанудың ықтимал көздерін жою.

Жұмыс ортасында тұтану көзідері:

- электр жабдықтарының ақаулары, сымдардағы, электр розеткалары мен ажыратқыштардағы ақаулар. Сондықтан, ақауларды уақтылы анықтау және жою, жоспарлы тексеріс жүргізу және барлық ақауларды уақтылы жою үшін өрттің алдын-алу өте маңызды;

- электр құрылғыларының ақаулығы. Өртті болдырмауға қажетті шараларға электр құрылғыларын уақтылы жөндеу, бұзылған электр құрылғыларын сапалы емес жөндеу кіреді;

- бөлмені ашық жылыту элементтері бар электр жылытқыштарымен жылыту. Қыздырылған беттердің шығуы өртке әкеледі, өйткені бөлмеде кітаптар, нұсқаулықтар және қағаз түріндегі қағаз құжаттары мен анықтамалықтар бар.

- жанғыш зат. Өрттің алдын алу үшін зертханада ашық жылыту құрылғыларын пайдаланбауды ұсынамын;

- сымдағы қысқа тұйықталу. Қысқа тұйықталу салдарынан өрт шығу ықтималдығын азайту үшін сымды жасырын істедім.

- Өрт қауіпсіздігі шараларын сақтамау және бөлмеде темекі шегу өрттің шығуына әкеледі. Лабораторияда темекі шегудің салдарынан болатын өртті жою үшін мен темекі шегуге үзілді-кесілді тыйым салуды және оған тек белгіленген жерде рұқсат етуді ұсынамын.

Өрт туындаған кезде алдымен электр қуатын өшіріп, өрт сөндіру бригадасын шақырып, эвакуация жоспарына сәйкес адамдарды бөлмеден шығарып, өрт сөндірушілермен өртті сөндіруге кірісу керек. Егер кішкене жалын болса, ауаны тұтату қондырғысына жетпеу үшін қолдағы құралдарды пайдаланылады.

4.2 Есептеу бөлімі

4.2.1 Жарықтандыру жүйесін есептеу бөлімі

Есеп әдістемелік нұсқауды негізге ала отырып орындалды [5].
Минималды жарықтандыруды Emin = 300 люкспен анықтайды.

Жарықтандыру жүйесін есептеу үшін біз кәдеге жарату әдісін қолданамыз. Бұл жұмыс бетінде қалыпты жарықтандыруды құру үшін шамдардың қажетті жарық ағынын анықтайды.

Жалпы жарық ағынын есептеу формуласы келесідей:

$$F_{\Sigma} = \frac{E_{\min} \cdot k \cdot S \cdot z}{\eta}, \text{ лм,}$$

мұнда E_{min} - ең төменгі жарық, люкс;

k - шамдардың ластануына байланысты жұмыс кезінде жарықтандырудың азаюын ескеретін қауіпсіздік коэффициенті; S - үй-жайдың ауданы, м2; z - орташа жарықтың ең аз жарықтандыруға қатынасы (флуоресцентті лампалар үшін z = l, l); η - жарық ағынының пайда болуы.

Біздің жағдайда, люминесцентті лампалар үшін k = 1,5, z флуоресцентті лампалар үшін = 1,1 аламыз.

Пайдалану коэффициенті шам шамына, төбенің ρп, еден еденінің шағылысу коэффициенттеріне және формула бойынша анықталатын бөлме индексіне байланысты:

$$i = \frac{S}{h \cdot (A + B)},$$

мұндағы h - шамның жұмыс бетінен биіктігі (біздің жағдайда h = 1,8 м); A - бөлменің ұзындығы (A = 5.50), B - ені (B = 3.75 м), S - бөлменің ауданы, S = A * B.

і есептейміз:

$$i = \frac{5.5 * 3{,}75}{1.8 * (5.5 + 3{,}75)} = \frac{20{,}625}{16{,}7} = 1.24$$

Төбенің шағылысу коэффициенттерін ρп = 70%, қабырғалары ρс = 50%, еденнің едені = 30% және LSPO-2 шамының түрін ескере отырып, біз пайдалану коэффициентін η = 0.60 анықтаймыз.

Жарық ағынының формуласындағы сандарды алмастырамыз, мынаны аламыз:

$$F_{\Sigma} = \frac{300*1.5*1.1*20.625}{0,6} = \frac{1361.5}{0.6} = 17015.63$$ (лм)

Бұл жарықтандыруды 6 LTB40 шамдармен қамтамасыз ете алады (өйткені осы типтегі әр шам 3000 лм шамға дейін жарық береді. Осы шартты орындау үшін L201G240-02M типті лампаларды пайдалану ұсынылуы мүмкін.

Біз бүкіл жарықтандыру жүйесінің электр қуатын есептейміз. Формуланы қолданамыз:

Ptot = P1 * N (W),

мұндағы P1 - бір шамның қуаты = 40 (Вт), N - шамдардың саны = 6.

Барлығы = 40 * 6 = 240 (Вт).

Тікелей жарық ағындары бар дисплей экрандарының сәулеленуінен ешқандай жарық болмауы үшін, жалпы жарықтандыру құрылғылары жұмыс орнының жағында, оператордың көру сызығына және терезесі бар қабырғаға параллель орналасқан. Арматуралардың мұндай орналасуы оларды дәйекті түрде қосуға және экспозицияның әсерінен көздердегі штаммды азайтуға мүмкіндік береді.

4.2.2 Желдету жүйесін жобалау

Есеп әдістемелік нұсқауларымен жүргізілді [6] Түтіктің мөлшерін есептеу үшін бастапқы мәліметтер ауа ағыны болып табылады (Гвент = 877 м3 / сағ) және бөлмедегі оның қозғалысының рұқсат етілген жылдамдығы - u. Әдетте өндірістік ғимараттардың желдету жүйелері үшін жылдамдықтың келесі таралуы қабылданады: бастың учаскелерінде 9-12 м / с, ал шеткі жағында 3-6 м / с. Біздің жағдайда u = 9 м / с аламыз.

Ауа өткізгіштің (воздуховод) қажетті ауданы f, m2 формула бойынша анықталады:

$$f_M = \frac{G}{3600*U} = \frac{877}{3600*9} = 0,027(\ ^2)$$

Бұл мән (желінің кедергісін анықтау кезінде желдеткіш пен электр қозғалтқышын таңдау кезінде) құбырдың ауданы ең үлкен стандартты мәнге тең болады, яғни f = 0,027 м. Содан кейін құбырдың көлденең қимасын есептеу құбырдың диаметрін анықтайды. F = 0,027 м ауданы үшін түтіктің шартты диаметрі d = 140 мм болатындығын анықтаймыз.

Желдету желісіндегі қысымның жоғалуын анықтаңыз. Желіні есептеу кезінде желдету қондырғыларындағы қысымның жоғалуы бақыланады. Механикалық желдету жүйелеріндегі табиғи қысым еленбейді. Жеткізуді қамтамасыз ету үшін желдеткіш ауа өткізгіштеріндегі қысымның кем дегенде 10% -ынан асатын қысым жасауы керек.

Желілік бөлімнің кедергісін есептеу үшін формула қолданылады:

$P = R * l + \xi * \frac{v^2 * p}{2}$ мұндағы R - желі бөліміндегі үйкеліс қысымының нақты жоғалуы, (R = 18 Па / м); l - түтік қимасының ұзындығы, м, l = 2,7 м; F - түтік бөліміндегі жергілікті жоғалту коэффициенттерінің қосындысы: 0,21 - шынтақ үшін, 0,05 - түзу қима үшін, 1,2 - кіретін тор; v - түтік қимасындағы ауа жылдамдығы, 9 м / с; p - ауаның тығыздығы (p = 1,2 кг / м).

Мәндерді формулаға қоямыз:

$P = 18 * 2,7 + 1,46 * \frac{9^2 * 1,2}{2} = 48,6 + 71 = 119,6$ (Па)

Желдеткіштің желінің күтпеген қарсыластығының 10% мөлшеріндегі шегін ескере отырып жасайтын қажетті қысымы:

Ptr = 1.1 * Pmax = 1.1 * 119.6 = 131.56 (Pa)

Ауаны басқару қондырғыларында төмен қысымды (1 кПа дейін) және орташа қысымды (1 ден 3 кПа дейін) желдеткіштер қолданылады. Кедергісі аз 200 Па дейінгі желілерде осьтік желдеткіштер қолданылады. Жанкүйерлер аэродинамикалық сипаттамаларға сәйкес таңдалады, яғни. Желдеткіштің жалпы сыйымдылығы (Rtr, Па) мен сыйымдылық арасындағы тәуелділік (Gtr, м3 / сағ).

Қосымша ысыраптарды немесе түтіктердегі ауаның сорылуын ескере отырып, желдеткіштің қажетті өнімі 10% артады, сондықтан:

Gtr = 1.1 * Gvent = 1.1 * 877 = 964.7 (м / сағ)

Анықтамалық мәліметтерге сәйкес біз қажетті желдеткіш пен электр қозғалтқышын анықтаймыз: желдеткіш O6-300 (N4), желдеткіштің тиімділігі J = 0,65.

Электр қозғалтқышының қуаты (N, кВт) мына формула бойынша есептеледі:

$N = \frac{G_{TP} * P_{TP}}{3,6 * \eta_B * \eta_{PП} * 10^6} = \frac{964,7 * 131,56}{3,6 * 0,65 * 10^6} = \frac{156582,7}{2,34 * 10^6} = 0,054$

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.

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.

Көптеген жағдайларда жинақталған деректер мен тәжірибені пайдалана отырып, одан әрі сандық мәндер түрінде өзгертілуі мүмкін қарапайым сөздік тұжырымдар түріндегі тәуекел салдарларының ықтималдығын бағалауға болады.

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

Тәуекелдің сөздік сипаттамасын немесе сандық интервалды пайдалана отырып, ұқсас кестелердің көмегімен тәуекелдің ықтималдығына баға беруге болады. Бағалау жүргізу кезінде тәуекелдердің әрқайсысы үшін мәндердің бір аралығын пайдалану қажет, әрі қарай олардың әрқайсысынан жұмыс басымдығын анықтау үшін.

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

Жоғарыда көрсетілген әр залалдың сипаттамасына қарай

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
2.3	SQL-инъекция	SQL сұраулары үшін сүзгілеу	3	Веб-қолданбаның желіаралық	0

		ережелерінің дұрыс еместігі		экраны	
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
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

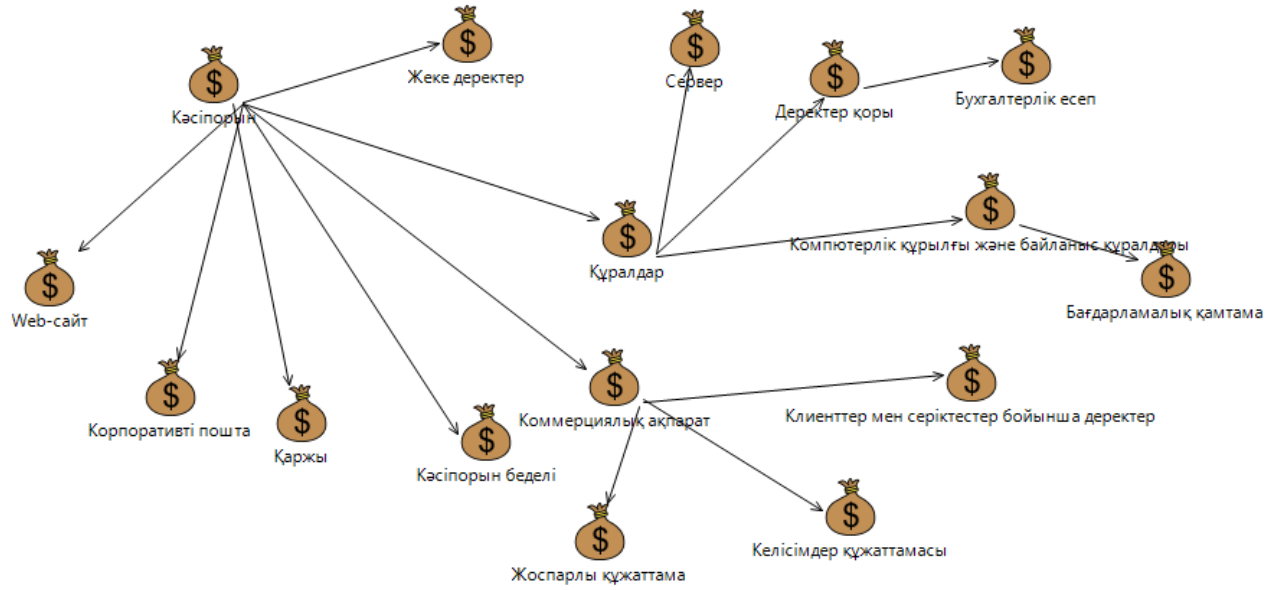
4.3	Деректерді ұстау	Бастапқы және ресурстық IP адрестерін алмастыру мүмкіндігі	4	Деректер мен пакеттерді жинайтын және талдайтын желідегі машинаны анықтайды	3
5 Сервер					
5.1	Серверді рұқсатсыз басқару	Қол жеткізу құқықтарын дұрыс бөлмеу	8	Рұқсат етілмеген қолжетімділікті жүзеге асыру мүмкіндігін 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.

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.



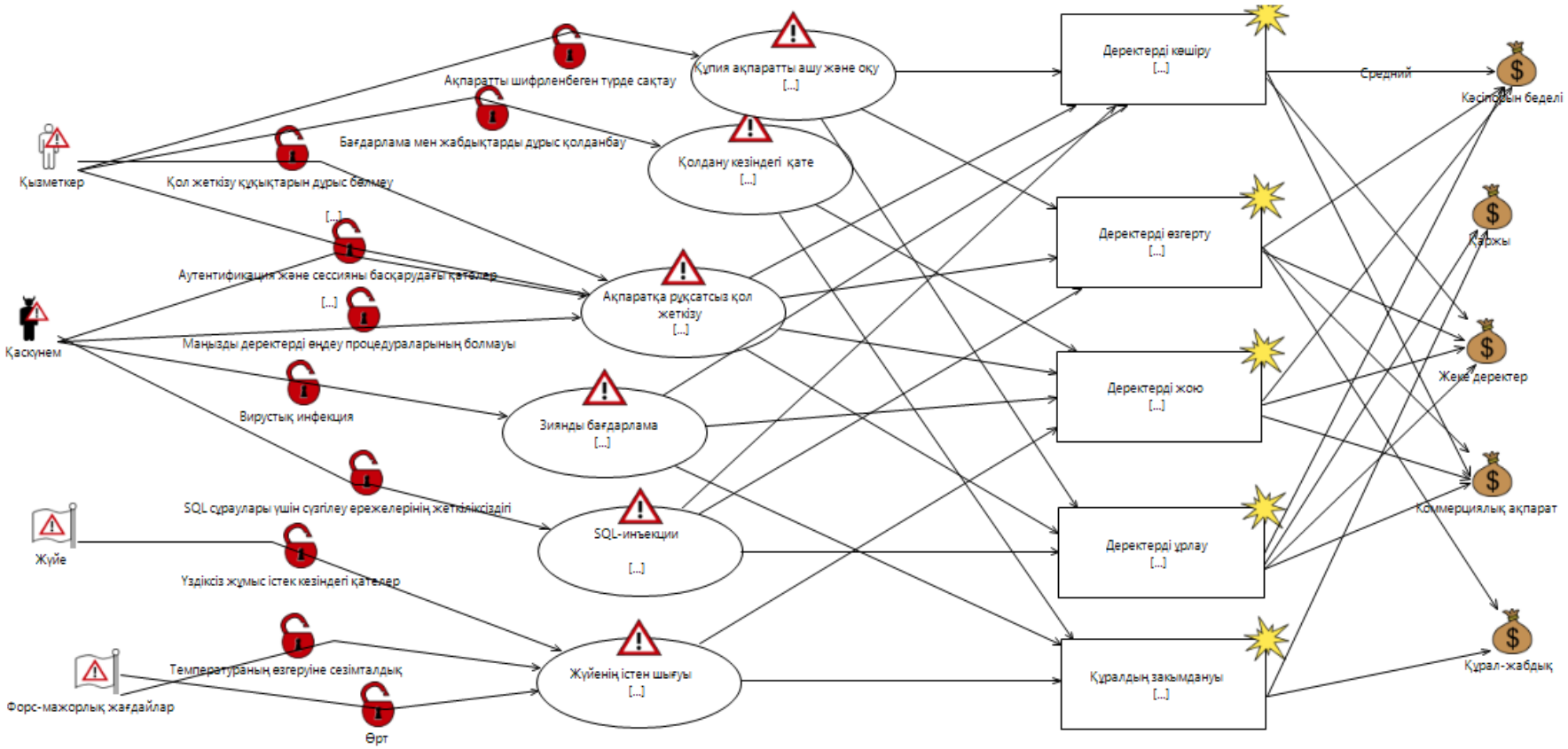
5.1-сурет – Активтер диаграммасы

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

Бағдарлмада келесі элементтер пайдаланылады:

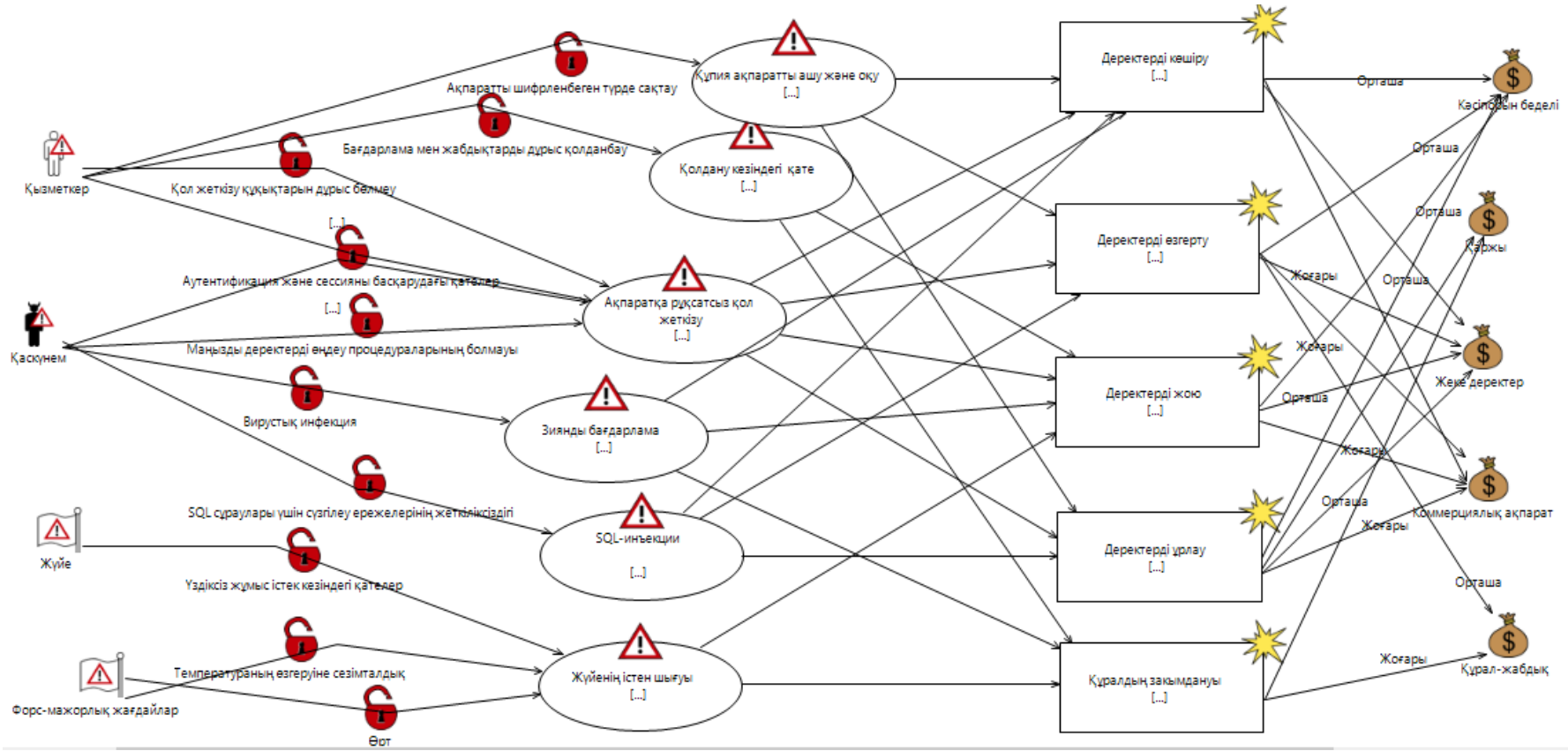
- Threat Human Accident - адам факторымен байланысты қасақана емес қауіп-қатерлерді белгілеу үшін
- Threat Human Deliberate - адам факторына байланысты қасақана қауіп-қатерлерді белгілеу үшін
- Threat Non Human адам факторымен байланысты емес қауіптерді белгілеу үшін;
- Threat Scenario - қатерлерді сипаттау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

5.4-кестені пайдалана отырып, қауіптер моделін жасаймыз. Тәуекелдер диаграммасын генерациялаймыз, бұдан әрі әрбір актив үшін әрбір тәуекел бойынша осы тәуекел жүзеге асырылған жағдайда салдарларды анықтаймыз. Алынған диаграмма 5.4 суретте көрсетілген.



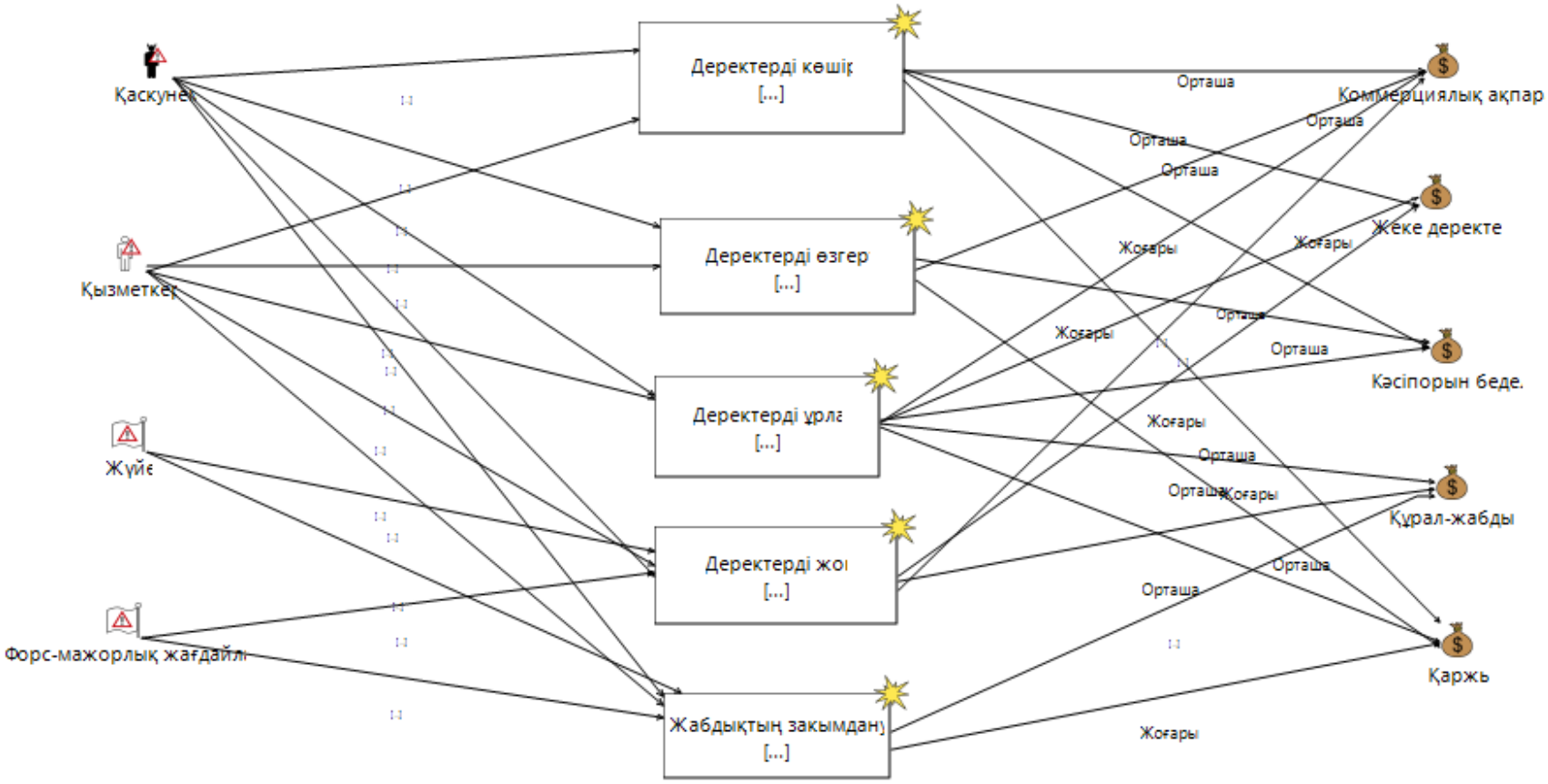
5.2-сурет–Қауіптер моделі

Бұдан әрі пайда болған тәуекелдерді іске асыру жиілігін анықтаймыз (белгілі бір уақыт кезеңінде қауіп-қатерді іске асырудың күтілетін саны). Әрбір актив үшін өмірлік цикл кезеңінде әрбір қауіптің туындау ықтималдығын белгілейміз.



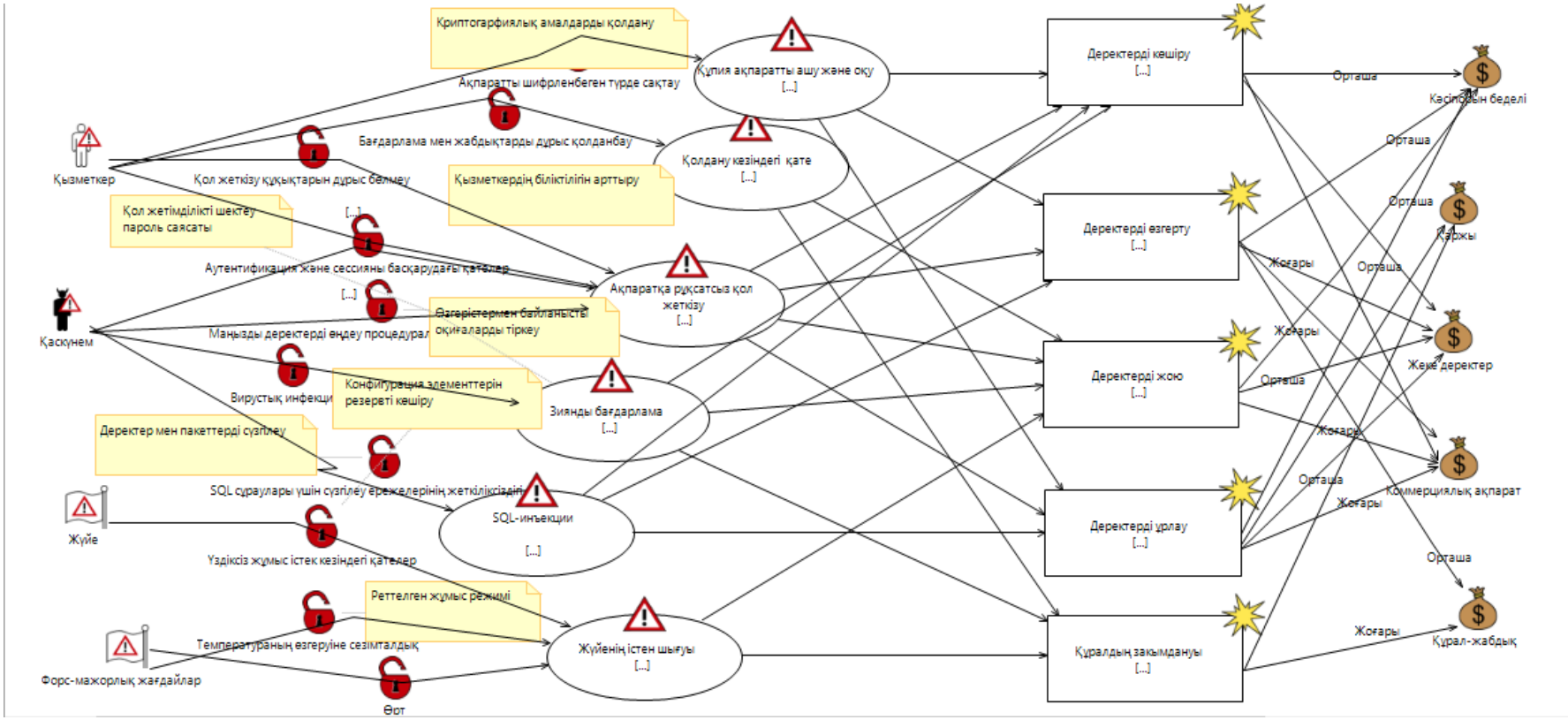
5.3-сурет – Ықтимал сипаттамалары бар қауіптер моделі

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)



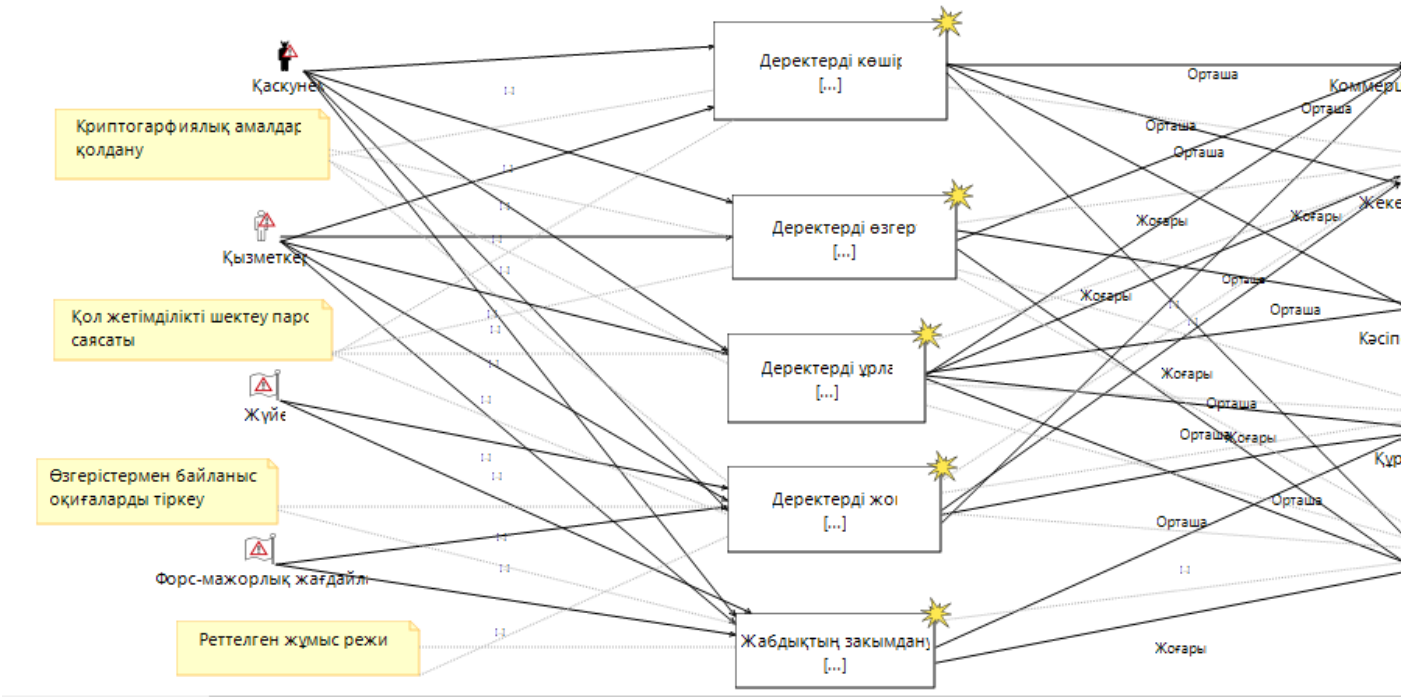
5.4-сурет – Қауіпті жүзеге асыру салдарларының сипаттамасы бар тәуекелдер диаграммасы

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 (сурет. 5.6).



5.6 –сурет – Қолайсыз тәуекелдер диаграммасы

ҚОРЫТЫНДЫ

Бұл дипломдық жұмыста «әлеуметтік инженерия ақпараттық қауіпсіздік аспектісінде» пәні бойынша зертханалық жұмыстар әдістемесін әзірлеп және қорғану амалдары ұйымдастырылды. Ол үшін әлеуметтік инженерияны зерттеу туралы мақсат қойылды. Әлеуметтік инженерияның зерттелуінің себебі, әлеуметтік инженерия - бүгінгі таңда, өте актуальді мәселенің бірі болып табылады. Әлеуметтік инженерия қаруларын, атап айтқанда: фишинг, претекстинг, фарминг, трояндық ат, кері әлеуметтік инженерияны жеке-жеке зерттеліп, оның шабуылының алдын алу амалдары қарастырылды. Зардап шегуші тек қана жеке адам емес, орта және үлкен компаниялар зардап шегуші рөлінде болуы мүмкін екендігі көрсетілді. Әлеуметтік инженерия қаруларынан қорғану немесе алдын алу мақсатында, эксперттердің жазған кеңестері оқылып, оған тұжырымдамалар жасалынды.

Әлеуметтік инженерия қарулары амалдарынан қорғану мақсатында, бірнеше алдын алу әдістері ойлап табылды. Мысалы, қызметкерлердің әлеуметтік инженерия туралы біліктілігін тексеру мақсатында бірнеше тесттер жасалды, Тест AnsTester платформасында жасалынды. Сонымен қатар, фишингтардан, вирустардан қорғану үшін антивирустық бағдарламалар (Trend Micro Internet Security) ұсынылып, қорғану әдістерінің қадамын көрсеттік, ойлап тапқан амалдарды түбегейлі қарастырып, жүзеге асатынына көз жеткіздік.

Сонымен қатар, қызметкерлерді әлеуметтік инженериядан қорғану мақсатында тренинг жасалынды және «социометрия» әдісі қолданылды Бұл әдіс жанама сұрақтар қою арқылы , әлеуметтік инженериялық шабуылға қарсылық білдіруге анықтауға, қызметкерлердің әлеуметтік инженериялық шабуылға қарсылық білдіруге білімінің қаншалықты екенін білуге мүмкіндік береді. Мұндай тәсілдердің құндылығы сол, әлеуметтік инженериялық шабуылға қарсылық білдіруге мінездерінің тұрақтылығын анықтауға мүмкіндік береді.

Жоғарыда көрсетілген қорғану жолдары , әлеуметтік инжнериялық шабуылдардың алдын алуға аз да болса өз әсерін тигізеді және амалын көрсететіні дәлелденді.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1 Кевин Митник, Искусство обмана / Компания АйТи; 2004.

2 Кузнецов М.В. Социальная инженерия и социальные хакеры/ СПб.:
БХВ-Петербург,2007.

3 Кевин Митник.. Искусство вторжения: Компания АйТи; 2004..

4 Социальная инженерия //Электронды мәлімет көзі. Элек.журн. EFSOL жүйе интеграциясы 2017. Мәліметке қол жеткізу : https://narfu.ru /agtu /www . agtu.ru

5 Социальная инженерия //Электронды мәлімет көзі. Элек.журн. Ярослав Бабин 2018. Мәліметке қол жеткізу : https://xakep.ru

6 Фишинг-атаки //Электронды мәлімет көзі. Элек.парақ. Владимир Безмалый 2008. Мәліметке қол жеткізу : https://www.osp.ru

7 Как взломать человека //Электронды мәлімет көзі. Элек.парақ. COSSA агентілігі 2017. Мәліметке қол жеткізу : https://www.cossa.ru

8 What is Social Engineering //Электронды мәлімет көзі. Элек.парақ. Robert Ikovly 2018. Мәліметке қол жеткізу : https://www.webroot.com

9 Social Engineering //Электронды мәлімет көзі. Элек.журн. Кевин Бивер2017. Мәліметке қол жеткізу : https://searchsecurity. Techtarget . com

10. Дюсебаев М.К., Абдимуратов Ж.С.. Промышленная вентиляция. Методические указания для выполнения курсовой работы для студентов специальности 5В073100 – «Безопасность жизнедеятельности и защита окружающей среды».- Алматы: АУЭС, 2013 - 26 с.

11. 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.

12. Жандаулетова Ф.Р., Бегимбетова А.С. Безопасность жизнедеятельности. Защита от производственного шума. Методические указания к выполнению дипломного проекта, Алматинский институт энергетики и связи. – Алматы, 2010.