ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ақпараттық және телекоммуникациялық технологиялар институты

«Киберқауіпсіздік, Ақпаратты Өңдеу және Сақтау» кафедрасы

Орналиев Алмат Канатулы

«BYOD саясатын қолданып корпоративтік желілерден деректердің ағып кетуінен қорғау»

Дипломдық жоба

ТҮСІНІКТЕМЕЛІК ЖАЗБА

5В100200 – «Ақпараттық қаупсіздік жүйелері» мамандығы

Алматы 2019

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ақпараттық және телекоммуникациялық технологиялар институты

«Киберқауіпсіздік, Ақпаратты Өңдеу және Сақтау» кафедрасы

ҚОРҒАУҒА ЖІБЕРІЛДІ
Кафедра меңгерушісі,
т.ғ.к., ассистент-
профессор
_____ Н.А.Сейлова
«_13_» _05_____2019 ж.

Дипломдық жобаға
ТҮСІНІКТЕМЕЛІК ЖАЗБА

Тақырыбы: «BYOD саясатын қолданып корпоративтік желілерден деректердің ағып кетуінен қорғау»

Мамандығы 5В100200-Ақпараттық қаупсіздік жүйелері

Орындаған Орналиев А.К.

Пікір беруші

«Қазтелепорт» АҚ

Басқарушы директор

_____ Төлеулиев С.Б.

«_06_» _05_____ 2019 ж.

Ғылыми жетекші

Сениор-лектор

_____ Иманбаев А.Ж.

«_13_» _05_____2019 ж.

Алматы 2019

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ақпараттық және телекоммуникациялық технологиялар институты

«Киберқауіпсіздік, Ақпаратты Өңдеу және Сақтау» кафедрасы

5В100200- Ақпараттық қаупсіздік жүйелері

БЕКІТЕМІН
Кафедра меңгерушісі,
т.ғ.к., ассистент-
профессор
_____Н.А.Сейлова
«__13__» ___05_____2019 ж.

Дипломдық жобаны орындауға
ТАПСЫРМА

Білім алушы *Орналиев Алмат Канатулы*
Тақырыбы: *«BYOD саясатын қолданып корпоративтік желілерден деректердің ағып кетуінен қорғау».*
Университет Ректорының *2018 жылғы «16» қазандағы №1162-б* бұйрығымен бекітілген.
Аяқталған жұмысты тапсыру мерзімі *20__жылғы «__»___*
Дипломдық жобаның бастапқы берілістері: *BYOD қорғау деңгейін арттыру, қарастырылмаған қоғау шараларындағы осалдықтар мен кемшіліктерін анықтау*
Дипломдық жобада қарастырылатын мәселелер тізімі
1. Теориялық бөлім
2. Практикалық бөлім
3. *Қосымша*
Сызба материалдар тізімі (міндетті сызбалар дәл көрсетілуі тиіс)
Сызба материалдары ___слайдта көрсетілген
Ұсынылған негізгі әдебиет *7 атаудан тұрады*

Дипломдық жобаны дайындау

КЕСТЕСІ

Бөлім атауы, қарастырылатын мәселелер тізімі	Ғылыми жетекші мен кеңесшілерге көрсету мерзімі	Ескерту
Теориялық бөлім	16.03.2019-26.03.2019	
Практикалық бөлім	07.04.2019-28.04.2019	

Дипломдық жобабөлімдерінің кеңесшілері мен норма бақылаушының аяқталған жобаға қойған

қолтаңбалары

Бөлімдератауы	**Кеңесшілер аты, әкесінің аты, тегі (ғылымидәрежесі, атағы)**	**Қол қойылған күні**	**Қолы**
Норма бақылау	Зиро А.А.	13052019	

Ғылыми жетекшісі Иманбаев А.Ж.

Тапсырманы орындауға алған білім алушы Орналиев А.К.

Күні «13» 05 2019 ж.

АҢДАТПА

Мақсаты: BYOD қорғау деңгейін арттыру

Міндеттері:

1. BYOD қорғаудың қолданыстағы тәсілдері мен шешімдерін талдау.
2. Қарастырылған қорғау шараларындағы осалдықтар мен кемшіліктерді анықтау.
3. BYOD қауіпсіздігін бұзуға қабілетті бар өнімдерді анықтау.
4. BYOD қорғау деңгейін арттыру арқылы табылған осалдықтардың алдын алу.

Дипломдық жоба 3 бөлімнен және қосымшадан, 56 беттен, 3 кестеден және 22 әдебиеттен тұрады.

Бірінші бөлімде MDM класындағы шешімдердің кемшіліктеріне талдау жүргізілді.

Екінші бөлімде мобильді құрылғылардан құпия деректерді ұрлауға шолу және талдау жасау үшін Observer бағдарламасы анықталып, компрометацияланатын құрылғыға орнатылды.

Үшінші бөлімде BYOD құрылғыларды кешенді қорғау стратегиясы сипатталады.

Қолданбада MDM шешімі үшін берілетін салыстыратын бағдарлама кестесінің кеңейтілген нұсқасы көрсетілген.

АННОТАЦИЯ

Цель: повышение уровня защищенности BYOD

Задачи:

1. Анализ существующих способов и решений защиты BYOD.
2. Выявление уязвимостей и недостатков в рассмотренных мерах защиты.
3. Определение существующих продуктов способных нарушить безопасность BYOD.
4. Предотвращение найденных уязвимостей повышением уровня защищенности BYOD.

Дипломный проект состоит 3 частей и приложений, 56 страниц, 3 таблиц и 22 источников литературы.

В первой части был проведен анализ недостатков решений класса MDM.

Во второй части обзор и анализ средств кражи конфиденциальных данных с мобильных устройств был определен параметр для проведения анализа и установлена программа Observer на компрометируемое устройство.

В третьем разделе описывается комплексная стратегия защиты BYOD устройств.

В приложении показана расширенная версия таблицы сравнивающая программы предоставляемые для решения MDM.

ABSTARCT

Purpose: to increase the level of security BYOD

Objective:

1. Analysis of existing methods and security solutions for BYOD.
2. Identification of vulnerabilities and shortcomings in the considered protection measures.
3. The definition of the existing products can compromise the security of BYOD.
4. Preventing found vulnerabilities by increasing the security level of BYOD.

The diploma project consists of 3 parts and annexes, 56 pages, 3 tables and 22 sources of literature.

In the first part the analysis of shortcomings of solutions of MDM class was carried out.

In the second part of the review and analysis of means of theft of confidential data from mobile devices, the parameter for the analysis was determined and the Observer program was installed on the compromised device.

The third section describes a comprehensive security strategy for BYOD devices.

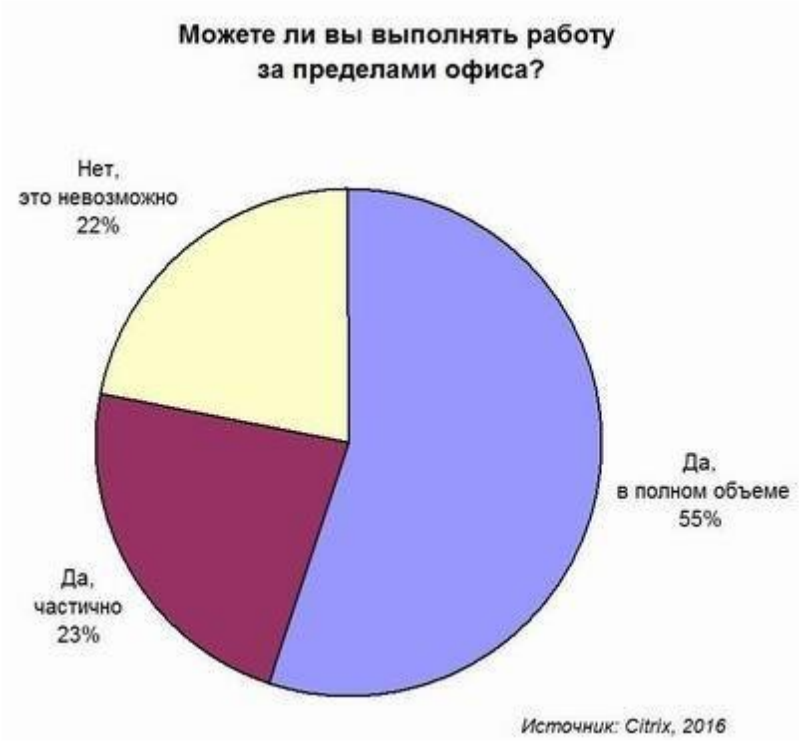
The Appendix shows an extended version of the table comparing the programs provided for the MDM solution.

МАЗМҰНЫ

Мазмұны	8
Кіріспе	9
1 БӨЛІМ. MDM шешімдерінің кемшіліктерін табу	11
1.1 MDM шешімдері	11
1.2 MDM шешімдерін салыстырмалы талдауы	14
1.3 Қорытындылар	19
2 БӨЛІМ. Мобильді құрылғылардан құпия деректерді ұрлау құралдарын шолу және талдау	21
2.1 Талдау жүргізуге параметрлерді анықтау	21
2.2 Құпия ақпаратты ұрлауға арналған бағдарламаларды шолу және талдау	21
2.3 Observer бағдарламасын орнату	25
2.4 Қорытындылар	27
3 БӨЛІМ. BYOD кешенді қорғау стратегиясын талдау	29
3.1 Деректердің ағып кетуін болдырмау	29
3.2 Виртуалды Windows ортасы	30
3.3 Терминалдық сессиялар	31
3.4 BYOD формуласы	35
3.5 Қорытындылар	37
Қорытынды	39
Пайдаланылған әдебиеттер тізімі	40
Қосымша А	41

КІРІСПЕ

Қазіргі әлем үрдісінде оның ажырамас бөлігі адам ұтқырлығы болып табылады. Әр түрлі кәсіпорындардың қызметкерлері мобильді болу үшін өз құрылғыларын: смартфондарды, планшеттерді, ноутбуктерді жұмыс мақсатында пайдалануға мәжбүр. BYOD - Bring Your Own Device тұжырымдамасы бар – "өз гаджетіңді алып кел", ол соңғы уақытта жұмыс берушілер жиі қолдана бастады, талдаушылардың айтуынша, жақын арада бұл үрдіс жаһандық ауқымға ие болады. Мәселен, 2018 жылы Citrix компаниясы ұсынған статистика бойынша сұралған компаниялар қызметкерлерінің 78% - ы толық немесе ішінара кеңседен тыс жерде жұмысты орындауға мүмкіндігі бар, тек 22% - ы алыстан жұмыс істей алмайды, көбінесе бұл жұмыстың ерекшелігіне байланысты.



1-сурет. BYOD саясатын пайдалану статистикасы.

Бұдан басқа, корпоративтік пайдалану үшін мобильді құрылғыларды сатып алуға ақша үнемдегісі келетін көптеген компаниялар олардың қызметкерлерінің жеке техникасын көбінесе өндіруші болып табылатын кәсіби мақсаттарда пайдаланатындығына ниеттеніп отыр. 2-суретте 2018 жылы Microsoft компаниясы жүргізетін және BYOD тұжырымдамасына әртүрлі елдердегі жұмыс берушілердің адалдық деңгейін анықтауға бағытталған зерттеулердің нәтижелері көрсетілген. Есеп қорытындысы бойынша BYOD пайдаланатын жұмыс берушілер арасында көшбасшы қытайлықтар.

2-сурет. BYOD саясатына жұмыс берушілердің көзқарас деңгейі.

Әрине, BYOD тұжырымдамасын қолдану кез келген уақытта, кез келген планетаның кез келген нүктесінен мәселелерді шешуге мүмкіндік береді, бұл, әрине, компанияның бәсекеге қабілеттілігін көптеген аспектілерде арттырады. Алайда, медальдің екінші жағы ақпараттық қауіпсіздік мәселесі болып табылады. Қарастырылып отырған тәсіл еңбек өнімділігін арттырады және компанияның IT – инфрақұрылымымен қызметкерлердің қанағаттануын арттырады, ақпаратты сақтау, беру, кәсіпорын желісін қорғау сияқты ақпаратты қорғауға байланысты бірқатар проблемалар туындайды. Қауіпсіздікті қамтамасыз ету үшін Mobile Device Management (MDM) класының шешімдерін жиі қолданады – ұялы құрылғыға арналған клиенттен (оны пайдаланушы мобильді қосымшалар дүкенінен жүктей алады), пошта трафигін және компания жағында басқаруға арналған серверді жіберуге арналған прокси-серверден тұратын бағдарламалық-аппараттық кешен. Осыған байланысты нарыққа BYOD қауіпсіздік мәселелерінің көптеген шешімдері ұсынылды. BYOD тұжырымдамасын қолдану кезінде корпоративтік желілерден ақпараттың жылыстауынан қорғау саласында жүргізілетін жұмыстардың өзектілігі осымен байланысты.

Зерттеудің мақсаты: BYOD қорғау деңгейін арттыру.

Зерттеу міндеттері:

1. BYOD қорғаудың қолданыстағы тәсілдері мен шешімдерін талдау.
2. Қарастырылған қорғау шараларындағы осалдықтар мен кемшіліктерді анықтау.
3. BYOD қауіпсіздігін бұзуға қабілетті бар өнімдерді анықтау.
4. BYOD қорғау деңгейін арттыру арқылы табылған осалдықтардың алдын алу.

1 БӨЛІМ. MDM КЛАСС ШЕШІМДЕРІНІҢ КЕМШІЛІКТЕРІН ТАЛДАУ

BYOD қауіпсіздігін қамтамасыз етудің ең көп таралған тәсілдерін қарастырайық, сондай-ақ әртүрлі коммерциялық ұйымдар ұсынатын қарастырылып отырған тәсілдердің тиімділігінің жеткіліксіз жағына дәлелдер келтіреміз.

1.1. Mobile Device Management (MDM)

Жоғарыда айтылғандай, Mobile Device Management (MDM) класының шешімдері – мобильді құрылғыға арналған клиенттен (оны пайдаланушы мобильді қосымшалар дүкенінен жүктей алады), компания жағында басқаруға арналған пошта трафигін және серверді беруге арналған прокси-серверден тұратын мобильді операциялық жүйелердің қауіпсіздігін қамтамасыз етуге арналған бағдарламалық-аппараттық кешен. Пайдаланушы өзінің ұялы құрылғысына клиенттік қосымшаны орнатқаннан кейін, ол корпоративтік деректерді – логин мен парольді енгізе отырып, авторизациялануы қажет. Қажетті параметрлер корпоративтік ресурстарға (мысалы, пошта клиентін баптау немесе VPN) кіру үшін құрылғыға жіберіледі. Сипатталған қадамдарды сәтті орындағаннан кейін, құрылғыны тіркеу туралы ақпарат әкімшілік тақтасында көрсетіледі. MDM жүйесі бұл құрылғы кімге тиесілі: қызметкер немесе компанияның өзі туралы түзетусіз мобильді құрылғыларды басқару мүмкіндігін ұсынады. Басқару әдетте қауіпсіздік саясаттарын қашықтан реттеу және оларды жаңарту ретінде жүзеге асырылады, құрылғы үшін маңызды ресурстармен қамтамасыз ету үшін конфигурацияларды орнату, деректер мен қолданбаларды тарату сияқты. Қорыта келе барлық алуан MDM шешімдерді айтуға болады, бұл жұмыс осы шешімдердің деңгейінде орын алады қосымшаларды пайдалана отырып, қашықтан басқару орталықтандырылған консоль[4]. Осыған орай, MDM класының шешімдері мобильді құрылғының клиенттік операциялық жүйесінің API-ін ұсынатын мүмкіндіктермен шектелген деп айтуға болады. Қарастырылып отырған сыныптың кейбір шешімдері "миналар" деп аталатын себехитрлік жамылғы бар – егер құпия мәліметтерді ашу қаупі туындаса, мобильді құрылғыдан барлық қосымшалар мен деректерді жояды. MDM шешімдерінің табысты қауіпсіздік бағыттары:

- сенімді құпия қорғаныс;
- қауіпсіздікке қауіп төнген жағдайда деректер мен қосымшаларды басқарылатын жою;
- кірістірілген жадты шифрлау немесе деректер мен қосымшаларды виртуалды "контейнерлеу".

Әрине, жоғарыда аталған барлық қасиеттер-MDM шешімдерінің күшті жағы, алайда, барлық осы функцияларды жүзеге асыру, әсіресе басқарылатын жою (бұл ең қиын функция) құрылғы желіде және жұмыс жағдайында болған

жағдайда ғана мүмкін. Басқа жағдайда MDM, Егер құрылғы жоғалған болса және ешкім таба алмаса, құрылғы біліксіз зиянкестердің қолына түскен болса немесе қалпына келтіру мүмкіндігінсіз физикалық үмітсіз жойылған болса, құпия деректердің сақталуын қамтамасыз етеді. Мұның бәрі, әрине, MDM шешімдері нақты қауіпсіздікке емес, сәттілікке негізделген деген ойға итермелейді. Қарастырылып отырған жүйе инсайдерлік қауіп-қатерден ешқандай қорғанысқа ие емес, тек болмашы кедергілер жасайды.

Тағы бір үлкен кемшілігі ол MDM-жүйелер болып табылады корпоративтік деректер шектелген қол жеткізу мүмкін емес қауіпсіз сақталуы BYOD құрылғыларда. BYOD-құрылғыларда корпоративтік деректерді сақтау MDM-жүйесі орнатылған немесе жоқ болғандықтан, ақпараттың ағу қаупін туындатады. Бір жағынан, Mobile Device Management кластары жүйесі шифрлау функциялары бар қосымшалар мен деректерді алыстан жою функцияларын біріктіре отырып, бұл проблеманы шешеді, алайда шын мәнінде бұл олай емес. Қол жетімділігі шектеулі деректер білікті мамандардың қолына түсіп, өзге тәсілмен ұрлануы немесе желілік арналар арқылы жіберілуі мүмкін. Мысалы, компанияда қызметкерлер өз девайстарын корпоративтік желіге қосу мүмкіндігіне ие болды, мұндай жағдайда деректерді BYOD-құрылғыға беру кезінде желі периметрі арқылы беру корпоративтік брандмауэр үшін көрінбейді. Қауіпсіздік келесі жаңылыстыруға болады, бұл шектеулі қолжетімділіктің корпоративтік деректерін BYOD-құрылғыларда қауіпсіз жасауға болады, алайда бұл солай емес, сондықтан. Жоғарыда келтірілген статистикада айтылғандай, қазіргі заманғы әлем үрдістерінде жаңа контентті құру үшін корпоративтік желі периметрінен тыс орналасқан жеке мобильді құрылғылар жиі пайдаланылады. Алайда, мұндай жағдайда компаниялар мен ұйымдарға жаңа контент жасайтын қызметкерлердің санасына сүйену және қызметкер жұмыс істерінің резервтік көшірмелерін жасайды немесе өз девайстарын корпоративтік деңгейде тиісті түрде резервтеу жүргізілетін жұмыс компьютерімен дер кезінде синхрондауды жүргізеді деп үміттену қажет. Егер жаңа корпоративтік деректер пайда болғаннан кейін қызметкер қадамдастыру немесе сақтық көшірме жасамаса, мобильді құрылғы жоғалады немесе ұрланған болады – жаңа жұмыс істелмеді деп санауға болады.

BYOD стратегиясы жұмыс мақсаттары үшін жеке мобильді құрылғыларды пайдалануды білдіргендіктен, көптеген адастырады, бұл BYOD-құрылғылар автоматты түрде құпия деректерге қол жеткізу керек. Әрине, қазір қызметкерге жеке мобильді девайстен бизнес-функцияларды орындауға мүмкіндік беретін көптеген түрлі шешімдер бар, бірақ бұл ең жақсы шешім емес. Когдапользователь өз құрылғысына қосымшаны орнатады, көбінесе ол кейбір пайдаланушы деректеріне қол жеткізуді сұрайды, бірақ пайдаланушылар көп жағдайда лицензиялық келісімді оқымайды, ал онымен бірден келіседі. Сіз де, сіздің ұйымыңыз да, орнатылған қосымшаның әзірлеушісі болып табылмайтындықтан, деректерді өңдеу қалай жүргізілетініне толық сенімді бола алмайды, ал жалпы біздің деректерімізді

өңдеу тәсілдері мен қауіпсіздігі туралы ешқандай ақпарат жоқ және осы процесті одан әрі бақылай алмаймыз. "Гартер" компаниясының зерттеулері бойынша iOS және Android басқаруындағы операциялық жүйелер нарықтың 94% - ын басып алды. "ПервыйБит" компаниясы жүргізген социологиялық зерттеулердің талдауынан IOS және Android пайдаланушылары үшінші тараптың қосымшаларын орнатуға көбірек бейім, оны Windows Phone пайдаланушылары туралы айтуға болмайды, алайда олардың үлесі мобильді платформалардың көшбасшыларымен салыстырғанда теңдесі жоқ. Сондай-ақ, зиянды бағдарламаны орнату мүмкіндігі гаджетке орнатылған қосымшалармен бірге өседі. Құпия ақпаратты әр түрлі сыртқы жинақтағыштарға, BYOD-құрылғылардан көшіріп ала алатын инсайдерлер туралы да ұмытуға болмайды. Қорғаныста кейбір MDM шешімдерінің бір бөлігі мобильді құрылғыларды бақылауды пайдаланады, пайдаланушыларға тек рұқсат етілген қосымшаларды орнатуға рұқсат етемін.

MDM-жүйелер DLP-жүйелеріне тең екенін өндірушілердің мәлімдемелері жиі кездеседі, олар олардың жүйелері құрылғыдағы құпия деректерді шифрлау және жою функцияларына ие екенін мәлімдейді. Алайда, MDM-жүйелерді DLP-жүйелермен салыстыру дұрыс емес, себебі салалық талдаушылар белгілеген қауіпсіздікке, Data Leak Privention терминінің анықтамаларына айтарлықтай айқын және назар аударылған. Жалпы қабылданған DLP анықтамаларын қарау кезінде-жүйе "берілетін деректер" (data-in-motion), "пайдаланылатын деректер" (data-in-use), және/немесе "сақталатын деректер" (data-at-rest) олардың мазмұны бойынша бірнеше жай-күйдегі деректерді талдауға тиіс. Алайда, MDM-жүйелер жоғарыда аталған деректер жай-күйін талдау үшін функцияларға ие емес, ал бұл функциялар деректердің тұтастығын, бақылау және мониторинг тапсырмаларын қамтамасыз етуде шешуші болып табылады. Бұдан басқа, Mobile Device Management класының жүйелері үшін инсайдерлік қауіп-қатерлерден және ақпараттың қасақана жайылмауынан жеткіліксіз қорғау мәселелері өзекті болып қала береді. Соңында, барлық MDM шешімдері олар орнатылған барлық мобильді құрылғыларға және оларда сақталатын құпия деректерге сенімді қатынауды пайдаланады, бұл дегеніміз, қосылатын ақпарат тасығыштарын және коммуникацияларды ақпараттың мазмұны бойынша, пайдаланушының контексті немесе деректер бойынша сүзуді қамтамасыз ету мүмкіндігі жоқ, бұл MDM өндірушілерінің мәлімдемелерінің шынайылығын жою-бұл DLP.

1.2 MDM шешімдерін ұсынушы компаниялардың салыстырмалы талдауы

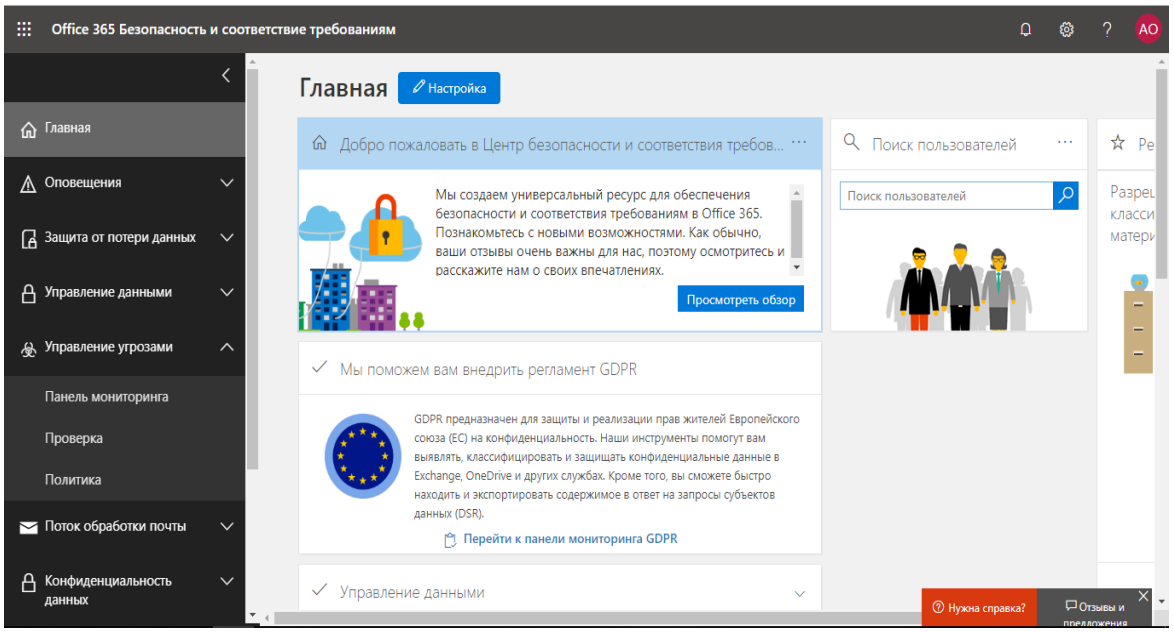
Атауы	Мобильді құрылғылар мен қосымшаларды басқару	Ақпаратты қорғау	Соңғы нүктенің масштабталуы	Жылдам жайылу	Бағасы тг/ай
Microsoft Intune	+	+	+	-	3191
IBM MaaS360	+	+	+	-	1517
Cisco Meraki	+	+	+	+	2836
VMware Airwatch	+	+	+	+	4130
MobileIron EMM	-	+	+	+	2653

1-кесте. MDM шешімдерін ұсынушы компаниялардың салыстырмалы талдауы

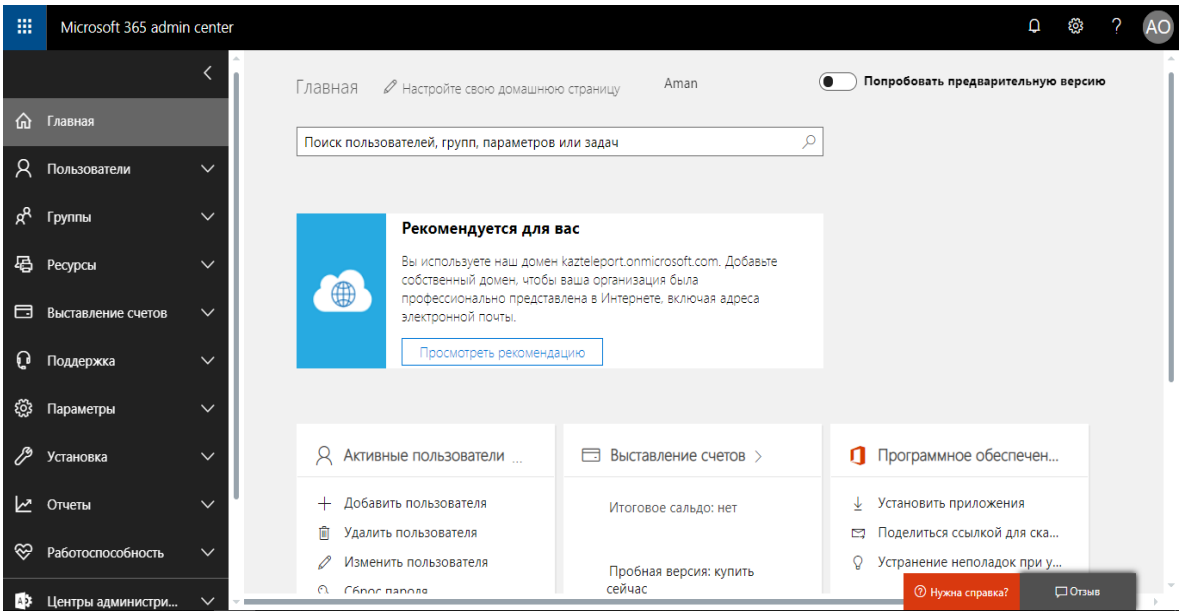
Әдетте MDM-шешім екі бөліктен тұрады: бақылау орталығы және клиенттік бағдарламалық қамтамасыз ету. Клиенттік бағдарламалық қамтамасыз ету пайдаланушының жеке ақпаратына қарамастан жұмыс деректерінің құпиялылығын қамтамасыз ететін шифрлау құралдарын, сондай-ақ құрылғыны қашықтан мониторингілеу мен басқаруға арналған бірқатар құралдарды қамтуы мүмкін.

20-дан аса MDM шешімдерін салыстыру мақсатында атақты кампаниялардың ұсынған тауарларын мобильді құралдар мен қосымшаларды басқару, ақпаратты қорғау, соңғы нүктенің мастабталуы, жылдам жайылу және баға секілді критерилер арқылы талдау жүргізілді. Кестенің толық нұсқасы А қосымшасында көрсетіледі. Жоғарыда қарастырылған талдауға сүйеніп ең оңтайлы нұсқа IBM компаниясы ұсынған MaaS360 шешімі деп шешіп, ары қарай тажирибе барысында осы тауар белгісін қолдану шешілді.

MDM шешімдерін ұсынатын компаниялар: Microsoft Intune



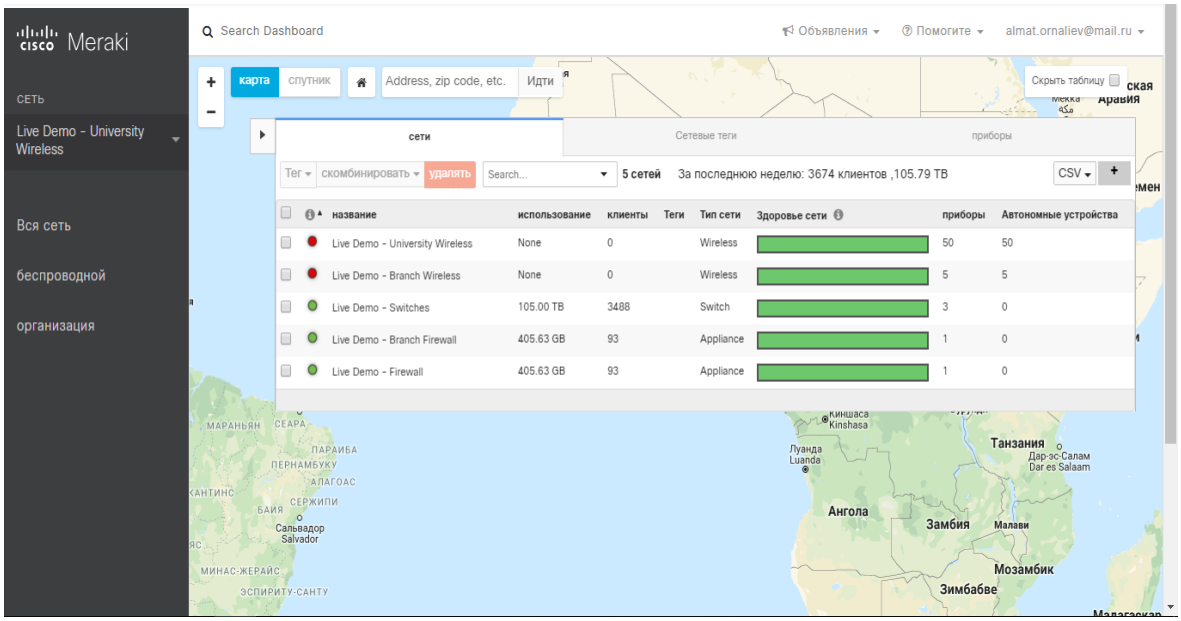
3-сурет. Бастапқы беті



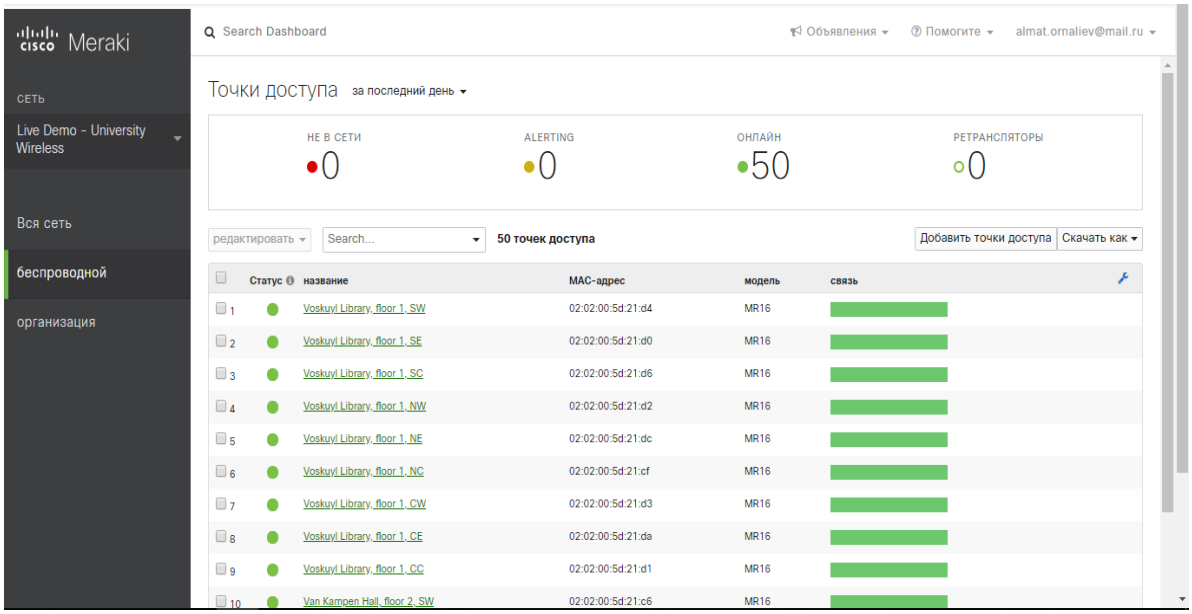
4-сурет. Басқару беті

Intune Enterprise Mobility + Security Microsoft компаниясына тиесілі. Intune Microsoft Azure әр түрлі шешімдерімен бірге қауіпсіздікті қамтамасыз ету және куәлікті басқару үшін порталдың жаңартылған жұмысын қамтамасыз етеді,бірақ әлі де ескірген әкімші функциялары бар. Intune сіздің әр түрлі мобильді экожүйені қолдау үшін әзірленген және бірыңғай біріздендірілген мобильді шешім iOS, Android, Windows және macOS құрылғыларын қауіпсіз басқаруға мүмкіндік береді.

MDM шешімдерін ұсынатын компаниялар: Cisco Meraki



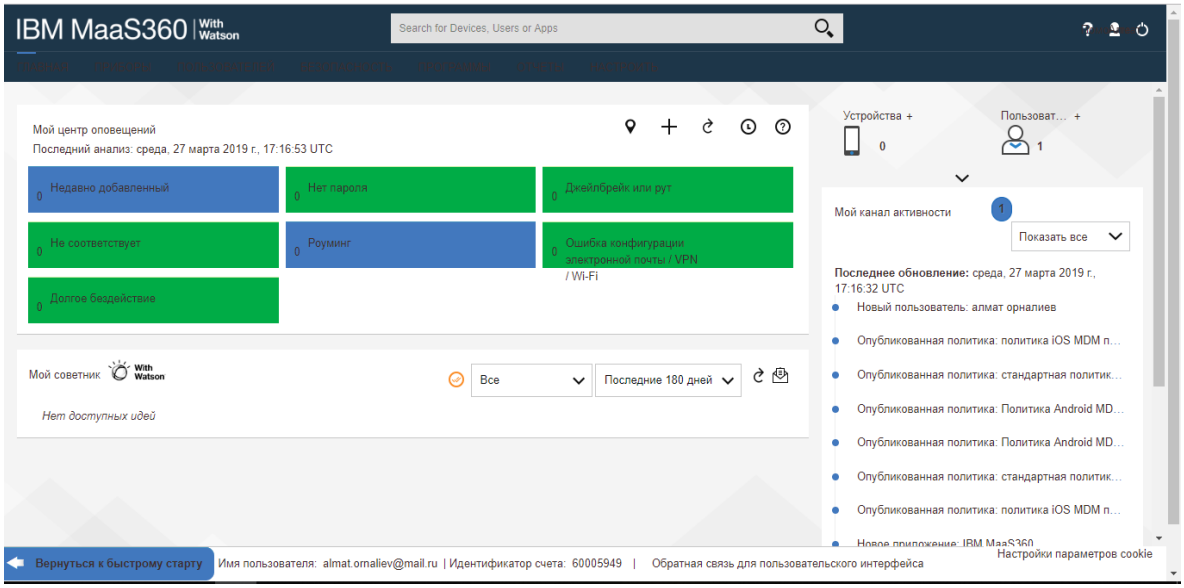
5-сурет. Бастапқы беті



6-сурет. Сымсыз байланысты тексеру

Cisco Meraki MDM шешімі мобильді құрылғыларды, Mac компьютерлерін, ДК және орталықтандырылған басқару панеліндегі бүкіл желіні біріздендірілген басқаруды қамтамасыз етеді. Ол сізге құрылғылардың қауіпсіздік саясатын сақтау, бағдарламалық жасақтама мен қолданбаларды өрістету, сондай-ақ мыңдаған басқарылатын құрылғыларда қашықтағы және жедел ақауларды жою үшін құрал береді.

MDM шешімдерін ұсынатын компаниялар: IBM MaaS 360



7-сурет. Басқару беті

IBM MaaS360 Watson-мен қоса сіздің бизнесіңіз үшін мобильді құрылғыларды басқару үшін шешім ретінде ұсынылады. Ол IOS, macOS, Android және Windows құрылғыларына интуитивті түсінікті портал арқылы көрнекілік пен бақылауды қамтамасыз етеді, ол MDM-ді артық ауыртпалық пен қиындықтарсыз барынша тиімді пайдалануға мүмкіндік береді.

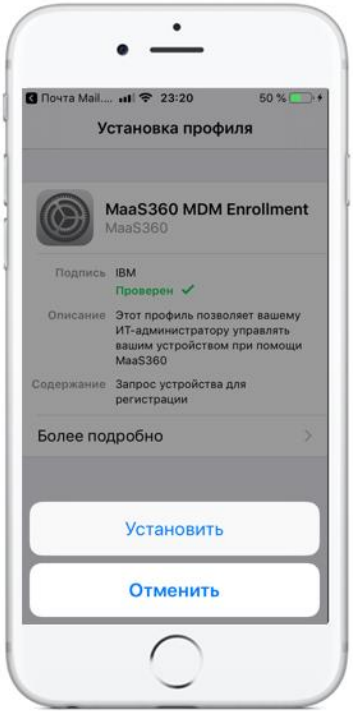
MaaS360-пен бірге, сіз Apple, Android немесе Windows құрылғыларымен жұмыс істеп жатқаныңызға қарамастан, соңғы нүктелерді қауіпсіз және тиімді түрде қамту мүмкіндігін беретін бір консольдан мульти-OS қолдауына ие боласыз. Ол бұл құрылғыны өзінің мүмкіндіктерінен тыс қорғай алады, соңғы пайдаланушыларды қауіпсіздікке нұқсан келтірмей, қажет нәрселермен қамтамасыз етеді.

Ерекшеліктері:

- Watson қозғалтқышымен жұмыс істейді;
- мульти OS және қауіпсіз платформа;
- Ios құрылғыларын қолдайды;
- Android үшін қорғалған құрылғылар мен бағдарламаларды қолдайды;
- Windows 10-дан Windows 7-ге дейін ескірген ДК қолдайды;
- корпоративтік мазмұнды сақтау үшін қауіпсіз контейнерді қамтамасыз етеді.

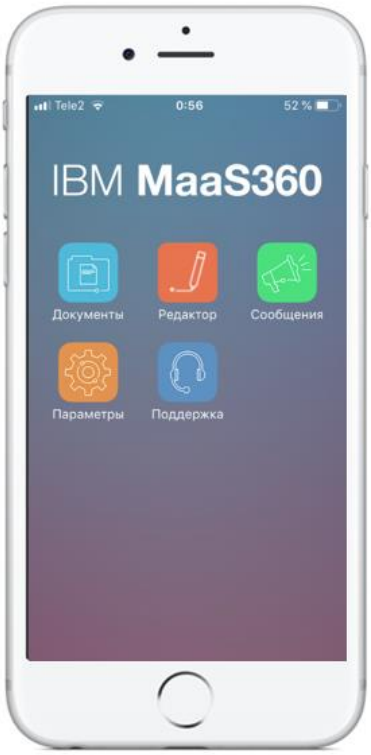
IBM MaaS360 шешімін орнату

Ол үшін Apple өнімдерін пайдаланушыларына AppStore желісінен, ал Android қолданушыларына PlayMarket желісінен IBM MaaS360 бағдарламасын жүктеп алу жеткілікті.



8-сурет. IBM MaaS360 орнатылуы

9-сурет. IBM MaaS360 орнатылуы



10-сурет. IBM MaaS360 орнатылуы

1.3. Қорытындылар

Жүргізілген талдау барысында келесі қорытындылар жасалды:

1. BYOD қауіпсіздік саласында жүргізілетін жұмыстар өзекті, себебі көрсетілген стратегияны пайдаланудың жылдам өсуі ақпараттың жылыстауы санының артуына алып келеді, ал ұялы құрылғыларды қорғау үшін ұсынылатын шешімдер олардың өндірушілері көрсеткеніндей тиімді емес. Mobile Device Management (MDM) шешімдер класы – әртүрлі вариациялары BYOD қорғау үшін пайдаланылатын мобильді операциялық жүйелердің қауіпсіздігін қамтамасыз етуге арналған бағдарламалық-аппараттық кешен қаралды.

2. Барлық артықшылықтарға қарамастан (шифрлеу, виртуалды контейнерлеу, басқарылатын жою, сенімді құпия қорғау) MDM маңызды кемшілігі бар – бұл құрылғы желіде және жұмыс істеп тұрған кезде ғана басқарылатын жою мүмкіндігі. Ал егер жоғары біліктілігі бар тәжірибелі зиянкестер оларға ие болса, онда құрылғыны желіден ажырату және құпия деректерді жоғалту ықтималдығы жоғары.

3. MDM өндірушілердің BYOD құрылғыларында құпия деректерді қауіпсіз жасау туралы мәлімдемесі дұрыс. Бекітудің дұрыстығы BYOD құрылғысын пайдаланушының мінез-құлқына байланысты. Мысалы, компанияда қызметкерлер өз девайстарын корпоративтік желіге қосу мүмкіндігіне ие болды, мұндай жағдайда деректерді BYOD-құрылғыға беру кезінде желі периметрі арқылы беру корпоративтік брандмауэр үшін

көрінбейді. Осыдан кейін қызметкер жұмыс уақытынан тыс уақытта корпоративтік желінің периметрінен тыс көрсетіледі және жоғалған немесе ұрланған жағдайда, зиянкестер олардың шифрланғанына қарамастан, деректерге қол жеткізе алады, мұның барлығы уақыт және еңбек шығыны. Сондай-ақ, BYOD-құрылғыларда жасалған деректердің резервтік көшірмелерін пайдаланушылар жиі жасайды ма, себебі резервтік көшірме және құрылғы болмаған жағдайда, жаңа атқарымдар ешқашан болған емес деп айтуға болады.

4. MDM-жүйелері DLP-жүйелеріне тең деп айтуға болмайды, өйткені MDM әртүрлі жағдайларда деректерді талдау функциялары жоқ және мобильді девайсқа MDM сенімді қол жеткізуіне байланысты пайдаланушының контексті бойынша, қосылатын сыртқы ақпарат тасығыштарын сүзу жоқ.

2-БӨЛІМ. МОБИЛЬДІ ҚҰРЫЛҒЫЛАРДАН ҚҰПИЯ ДЕРЕКТЕРДІ ҰРЛАУ ҚҰРАЛДАРЫН ШОЛУ ЖӘНЕ ТАЛДАУ

2.1. Талдау жүргізу үшін параметрлерді анықтау

Ұялы құрылғыларды қадағалайтын және құпия ақпаратты ұрлайтын бағдарламалық құралдарды қарастырайық. Талдау үшін басу пернелер комбинациясын сақтау функциясы, экран скриншот функциясы бар құралдарды таңдаймыз. Көрсетілген функцияларды орындау нәтижелерін бағдарлама Интернет желісін пайдалана отырып серверге беруі тиіс, яғни нәтиже алу үшін қаскүнемге компрометацияланатын құрылғыға физикалық қол жеткізудің қажеті жоқ. Талдау жүргізу кезінде бірнеше параметрлерді ескереміз:

- қолданба жасырын жұмыс, яғни, шпиондық бағдарлама пайдаланушы анықтау оқиға қаншалықты ықтимал;
- орнату күрделілігі, яғни зардап шегушінің құрылғысына шпиондық бағдарламаны орнату үшін қанша уақыт қажет;
- конфигурация қиындығы, қалаған деректерді дұрыс алу үшін бағдарлама конфигурациясы қаншалықты қиын және ұзақ орындалатынын ескереміз;
- бағдарлама жұмысы кезінде құрылғының тұтынылатын ресурстарының саны;
- шпиондық бағдарлама жұмысының нәтижесінде жиналған деректерді беру үшін тұтынылатын интернет-трафиктің саны;
- бағдарламаны антивирустық құралдармен табу мүмкіндігі.

Вирусқа қарсы құралдармен Шпион-бағдарламаны анықтау мүмкіндігін тексеру үшін талдау жүргіземіз, соның нәтижесінде тегін нұсқасы бар мобильді құрылғыларға арналған антивирус рейтингі анықталады. Бұл үшін сайт есебінің нәтижелеріне жүгінеміз comss.ru 2018 жылдың екінші тоқсанында сауалнама жүргізілген сауалнамаға 7000 респондент қатысты.

Мобильді антивирустық бағдарламалардың рейтингі 2-кестеде берілген.

Бағдарламаа аты	Әзірлеуші	Басып алу саны	Пайдаланушылар бағасы
CM Security Antivirus & AppLock	Cheetah Mobile	100 млн	4,7
Kaspersky Internet Security	«Лаборатория Касперского»	10 млн	4,6
ESET NOD 32 Mobile Security	ESET	1 млн	4,6
Avast Mobile Security & Antivirus	Avast Software	100 млн	4,5
360 Security	Qihoo 360	100 млн	4,5
Dr. Web v 12.0 Antivirus	Doctor Web	50 млн	4,5
McAfee Security & Antivirus Free	McAfee (Intel Security)	10 млн	4,5

2.2. Құпия ақпаратты ұрлауға арналған бағдарламаларды шолу және талдау

Amobile Spy компаниясының IKeyMonitor Mobile Spy-Android Және iOS басқаруындағы мобильді құрылғыларға арналған кейлоггер, енгізілген парольдерді басу, веб-браузерге кіру тарихын сақтау, скриншоттарды алу және жұмыс нәтижелерін электрондық поштаға немесе FTP-ға жіберу мүмкіндіктері бар. IKeyMonitor Mobile Spy бағдарламасын талдау үшін бағалау үшін бұрын орнатылған параметрлерді анықтаймыз.

- қолданба жұмысының жасырындылығы – қарастырылып отырған параметр IKeyMonitor Mobile Spy бағдарламасына сәйкес келмейді, өйткені есептегішті іске қосқан кезде Пайдаланушы құралды оңай табуы мүмкін, ол үшін тек қана аты бар бағдарлама;

- қолданбаны орнату күрделілігі-өндіруші сайтынан жүктелген орнату файлынан компрометацияланатын құрылғыға өте оңай және тез орнатылады;

- қолданба конфигурациясының күрделілігі – бағдарламаны сәтті теңшеу үшін теңшеу дұрыстығына сенімді болу үшін ұзақ уақыт жұмсау қажет. Сонымен қатар, конфигурация кезінде қиындықтардың пайда болуын растау болып табылатын қосымшалардың жұмысқа қабілеттілігін тексеру қажет;

- тұтынылатын ресурстар саны 32 МБ ЖЖҚ, 86 Мб ЖЖҚ;

- тұтынылатын интернет-трафиктің саны-деректер серверге жіберер алдында сығылады, ресурстар шығыны оңтайландырылды, сондықтан қазіргі уақытта пайдаланушы үшін Интернет-трафиктің шығыны байқалмайды;

- табу мүмкіндігі spy жолаушылар өтеді, сондықтан құралдарымен – зерттеу нәтижесінде бағдарлама табылды мынадай жолаушылар өтеді, сондықтан құралдарымен: CM AntiVirus Security & AppLock, Kaspersky Internet Security, Avast Mobile Security & Antivirus, ESET NOD 32 Mobile Security 360 Security, Dr..Web V. 12.0 Anti-virus.

Жүргізілген талдау нәтижесінде қорғау құралдарын сауатты пайдалану кезінде ikeymonitor Mobile Spy бағдарламасының көмегімен құпия ақпаратты ұрлау қаупі аз.

TolkLog-хат жазысуды, телефон қоңырауларын, сондай-ақ телефонның нақты уақыт режимінде орналасқан жерін бақылауға мүмкіндік беретін ұялы телефонды қашықтан бақылау қызметі. TolkLog бағдарламасын талдау үшін бағалау үшін бұрын орнатылған параметрлерді анықтаймыз.

- қолданба жұмысының жасырындылығы – қарастырылып отырған параметр TolkLog бағдарламасына сәйкес келмейді, өйткені тапсырма диспетчерін іске қосқан кезде пайдаланушы құралдың аты бар бағдарламаны оңай табуы мүмкін;

- қолданбаны орнату күрделілігі-өндіруші сайтынан жүктелген орнату файлынан компрометацияланатын құрылғыға өте оңай және тез орнатылады;

- тұтынылатын ресурстар саны 108 Мб ОЗУ 110 Мб ПЗУ;

- тұтынылатын интернет-трафиктің саны-деректерді қосымшамен беру сәтінде интернет беттерді жүктеу жылдамдығының төмендеуі байқалады, бұл компрометацияланатын құрылғының пайдаланушысын алаңдататын болады;

- антивирустық құралдармен Шпион-бағдарламаны анықтау мүмкіндігі-зерттеу нәтижесінде бағдарлама зерттеу жүргізу үшін іріктелген барлық антивирустық құралдармен анықталды.

Жүргізілген талдау нәтижесінде TolkLog бағдарламасының көмегімен құпия ақпаратты ұрлау қаупі жоқ деп айтуға болады.

Phone Control-кіріс/шығыс қоңыраулары, sms, mms және орналасқан жері логгер-бағдарлама. Android платформасында смартфонды қашықтан басқару, смартфон қызметінің мониторингі, жасырын логгер. Phone Control бағдарламасын талдау үшін бағалау үшін бұрын орнатылған параметрлерді анықтаймыз.

- бағдарлама жұмысының жасырындылығы-бағдарлама толық жасырын режимде жұмыс істейді, яғни пайдаланушының компрометациялайтын құрылғыны бағдарламалық жасақтаманы табу ықтималдығы-төмен;

- қолданбаны орнату күрделілігі – қолданбаны орнату үшін, стандартты қауіпсіздік жүйесін өшіру арқылы құрылғыда қосымша параметрлер жасау керек;

- тұтынылатын ресурстар саны-39 МБ ЖЖҚ, 65 Мб ЖЖҚ;

- тұтынылатын интернет-трафиктің саны-құрылғының пайдаланушысы үшін іс жүзінде көрінбейтін, өйткені бағдарламаның жұмысы барынша оңтайландырылған;

- табу мүмкіндігі spy жолаушылар өтеді, сондықтан құралдарымен – зерттеу нәтижесінде бағдарлама табылды мынадай жолаушылар өтеді, сондықтан құралдарымен: Kaspersky Internet Security, Avast Mobile Security & Antivirus.

Жүргізілген талдау нәтижесінде, Phone Control бағдарламасының көмегімен құпия ақпаратты ұрлау қаупі бар деп айтуға болады.

Shotic компаниясынан Mobile Spy Shot-Android операциялық жүйесінің басқаруымен мобильді құрылғыға Орнатылатын шпиондық бағдарлама. Бағдарлама функционалы зардап шегушіні қадағалау және құпия ақпаратты ұрлау үшін параметрлерді икемді реттеуге мүмкіндік береді. Интернет желісі арқылы серверге нәтижелерді жіберу мүмкіндігі бар. Mobile Spy Shot бағдарламасын талдау үшін бағалау үшін бұрын орнатылған параметрлерді анықтаймыз.

- қолданба жұмысының жасырындылығы – қарастырылып отырған параметр Mobile Spy Shot бағдарламасына сәйкес келмейді, өйткені, пайдаланушы тапсырманың тіркесімін іске қосқан кезде, пайдаланушы аты бар бағдарламаны оңай табуы мүмкін;

- қолданбаны орнату күрделілігі-өндіруші сайтынан жүктелген орнату файлынан компрометацияланатын құрылғыға өте оңай және тез орнатылады;

- тұтынылатын ресурстар саны 98 Мб ОЗУ 152 Мб ПЗУ;

- тұтынылатын интернет-трафиктің саны-деректерді қосымшамен беру сәтінде интернет беттерді жүктеу жылдамдығының төмендеуі байқалады, бұл компрометацияланатын құрылғының пайдаланушысын алаңдататын болады;

- табу мүмкіндігі spy жолаушылар өтеді, сондықтан құралдарымен – зерттеу нәтижесінде бағдарлама табылды мынадай жолаушылар өтеді, сондықтан құралдарымен: CM AntiVirus Security & AppLock, Kaspersky Internet Security, Avast Mobile Security & Antivirus, ESET NOD 32 Mobile Security 360 Security, Dr..Web V. 12.0 Antivirus.

Жүргізілген талдау нәтижесінде, қорғау құралдарын сауатты пайдалану кезінде Mobile Spy Shot бағдарламасының көмегімен құпия ақпаратты ұрлау қаупі аз.

Observer-құрбанның ұялы құрылғысынан құпия ақпаратты бақылау және ұрлауға арналған Spy бағдарламасы. Android операциялық жүйесінің басқаруындағы телефондарға да, планшеттерге да орнатылады. Бағдарлама оңай орнатылады және пайдаланушы үшін көрінбейтін барлық қажетті ақпаратты жазады және зиянкестерге интернет желісі арқылы нәтижені жібереді. Сондай-ақ, өндіруші iPhone, iPad, Windows PC, Windows Mobile, Mac сияқты құрылғыларға арналған бағдарламаны басқа операциялық жүйелерге бейімдеу бойынша жұмыстардың 50% - дан астамының орындалғанын мәлімдейді. Сонымен қатар, бағдарламаны орнату және конфигурациялау үшін арнайы білім және мобильді құрылғылармен жұмыс істеу тәжірибесі

талап етілмейді. Observer бағдарламасын талдау үшін бағалау үшін бұрын орнатылған параметрлерді анықтаймыз.

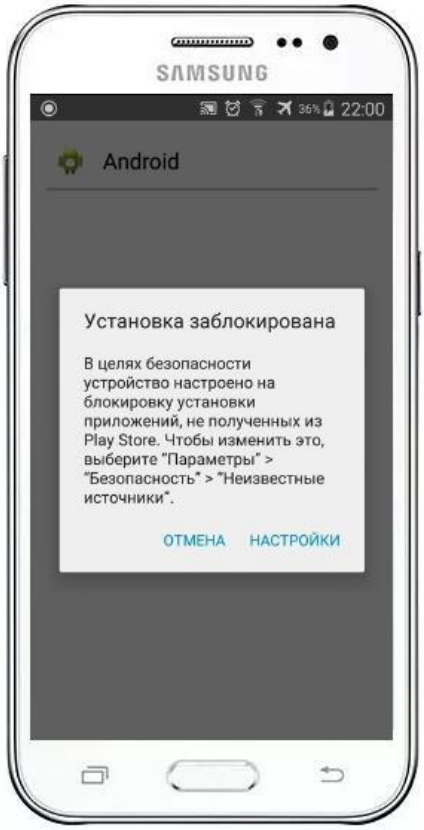
- қолданба жұмысының жасырын болуы – қарастырылып отырған параметр Observer бағдарламасына сәйкес келеді, себебі пайдаланушы тапсырмаларды реттеушіні іске қосқан кезде іс жүзінде мүмкін емес;
- қолданбаны орнату күрделілігі-өндіруші сайтынан жүктелген орнату файлынан компрометацияланатын құрылғыға өте оңай және тез орнатылады;
- тұтынылатын ресурстар саны 61 Мб ОЗУ 74 Мб ПЗУ;
- тұтынылатын интернет-трафиктің саны – құрылғыны пайдаланушы үшін ұрланған деректерді елеусіз беру қалады, өйткені бағдарлама мобильді интернетті пайдалану арқылы деректердің кішкентай пакеттерін береді, ал үлкен пакеттер Wi-Fi желісін пайдалану кезінде беріледі;
- антивирустық құралдармен Шпион-бағдарламаны анықтау мүмкіндігі – зерттеу нәтижесінде Бағдарлама жоғарыда анықталған тізімнен бірде-бір антивирус таппады. Сонымен қатар, Бағдарлама өндірушісі кез келген антивируспен Observer-ті "достау" мүмкіндігі бар екенін мәлімдейді.

Жүргізілген талдау нәтижесінде, қаралған бағдарламаны пайдалану кезінде, неғұрлым сауатты күйге келтіру жағдайында, компрометацияланатын құрылғыны пайдаланушы күдікті әсер пен ақпаратты ұрлауды таппайтыны анықталды. Рұқсат етілмеген әрекеттерді болдырмау үшін қосымша қорғау шараларын қабылдау қажет. Барлық қарастырылған бағдарламалардың ішінен Observer зерттеу тақырыбы бойынша үлкен қызығушылық танытатындықтан, оған толығырақ тоқталайық.

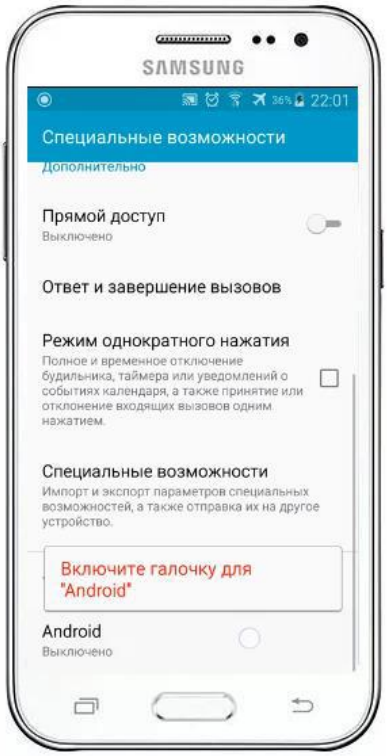
2.3. Observer бағдарламасын компромет ететін құрылғыға орнату

Ол үшін зардап шегушінің құрылғысын 2-3 минутқа қою керек, және бұл үшін root рұқсат қажет емес. Орнату және конфигурация өздігінен жасалады, сондай-ақ бағдарламаны әзірлеушіде бұрын аталған параметрлер бойынша құрылғыны өзі конфигурациялайтын құрт қосылған орнатушы файлға тапсырыс беру мүмкіндігі бар. Біз бірнеше минут құрбандық құрылғысын алу жағдайын қарастырамыз.

11-сурет. Observer бағдарламасын орнату



12-сурет. Observer бағдарламасын орнату



13-сурет. Observer бағдарламасын орнату

Жүргізілген эксперимент негізінде, зардап шегушінің құрылғысына Observer бағдарламасын орнату 2 минуттан аспайды деп айтуға болады. Қаскүнем үшін тапсырманы барынша қарапайым етеді. Бағдарлама сервері дәл осылай орнатылғандықтан, және де сыни параметрі жоқ - орнату уақыты, оның қондырғысын түсіндірме жазбада егжей-тегжейлі сипаттаудың мағынасы жоқ, орнату 2 минут алды деп айтуға ғана тұрарлық.

2.4. Қорытындылар

Жүргізілген талдау барысында келесі қорытындылар жасалды:

1. Ең танымал шпиондық бағдарламалар, ұялы құрылғылар үшін Android операциялық жүйесінің басқаруында жұмыс істейді.

2. Бағдарламалардың заңсыз әрекеттері сол немесе басқа тәсілдермен, көбінесе вирусқа қарсы құралдармен анықталады. Дегенмен, интернет-Observer желісінде еркін қатынайтын spy бағдарламасы бар. Көрсетілген бағдарлама 2018 жылғы статистика бойынша мобильді вирусқа қарсы ТОП құрамына кіретін барлық антивирустар үшін көрінбейді. Бағдарлама пайдаланушының рұқсатынсыз құпия ақпаратты зиянкестер алатын серверге жібереді. Бағдарлама Android астында Жасырынып, құрылғыдағы із қалдырмайды. Жүргізілген талдау негізінде 2-тарауда келтірілген BYOD қауіпсіздігінің стандартты формуласы жеткіліксіз деп айтуға болады. Құпия деректермен жұмыс істеу сессиясы кезінде 2-тарауда келтірілген барлық ұсыныстарды пайдалана отырып, деректердің жылыстауы құрылғы экранының скриншоттарын алу және серверге және одан әрі қаскүнемге

жіберу жолымен болуы мүмкін. Осы тарауда анықталған жолмен құпия ақпаратты ұрлауды болдырмау үшін BYOD қауіпсіздік формуласы жақсартылуы тиіс.

3 БӨЛІМ. BYOD КЕШЕНДІ ҚОРҒАУ СТРАТЕГИЯСЫН ТАЛДАУ

MDM класындағы шешімдердің кемшіліктерін талдау ұялы құрылғыларды басқару жүйесі кешенді сипатқа ие болатын кең қорғаныс стратегиясының бөлігі болуы мүмкін деп айтуға мүмкіндік береді. Жоғарыда қарастырылған жүйені деректерді шифрлау және басқару, жалпы мобильді құрылғыларды бақылау сияқты міндеттерді шешу үшін соңғы қорғаныс шарасы ретінде қолдану қажет. Тек осы жағдайда ғана мобильді контентті басқару жүйесінің жұмысы тиімді болады.

Корпоративтік деректерге қол жеткізу үшін пайдаланылатын мобильді құрылғылардың қауіпсіздігін қамтамасыз ету саласында ең тиімді болып табылатын vDLP (Virtual Data Leak Prevention) тәсілі бар. Әдістің мәні-пайдаланушы өзінің жеке мобильді құрылғысынан Компанияның корпоративтік деректеріне қашықтағы қосылу арқылы қол жеткізе алады. BYOD-құрылғы виртуалды Windows орталарына терминалдық сессиялар арқылы қашықтан қосылады. Windows-орталар, өз кезегінде DLP-жүйемен (Data Leak Prevention) қорғалады, ол хостада жұмыс істейді, соның арқасында бақыланбайтын деректердің кемуін болдырмайды.

3.1 Деректердің ағуын болдырмау

DLP жүйелерінде компаниялардың ақпараттық активтерінің олардың корпоративтік желісінен сыртқы ортаға шығуын болдырмауға бағытталған технологиялар пайдаланылады. Көрсетілген технологиялардан басқа DLP-жүйе қорғау мақсатына жету үшін бағдарламалық немесе бағдарламалық-аппараттық құралдарды қамтиды. DLP-жүйесін қорғайтын желі периметрін кесіп өтуге тырысатын деректер ағыны талдауға ұшырайды. Егер демодуляцияланған ақпарат ағынында құпия анықталса, онда жүйенің белсенді компоненті өз жұмысын бастайды және ақпарат блогын беруге тыйым салынады. Соңғы уақытта DLP-жүйелер ішкі, яғни инсайдерлік қауіптерге көп көңіл бөлінуінің арқасында, соңғы өткенге қарағанда, сыртқы қауіп көздеріне баса назар аударылды. Желі периметрлерінен тыс берілетін ақпарат құпия DLP-жүйе екі тәсілмен болуы мүмкін. Бірінші тәсілді пайдалану кезінде гриф, белгі сияқты құжаттардың формальды белгілеріне талдау жүргізіледі, алайда бұл әдіс контентті талдау жүргізілетін екінші тәсілге қарағанда олардың құпиялылығы мен құпиялылығын көрсету үшін барлық құжаттарды алдын ала өңдеуді талап етеді. Екінші тәсілді пайдаланған жағдайда жалған іске қосылуы мүмкін, бұл оның кемшілігі болып табылады, алайда, егер құжат белгіленбеген болса, құпия ақпараттың жария болу мүмкіндігі формальды белгілерді талдау тәсілінің кемшілігі болып табылады. Екінші әдіс өте тиімді, бірақ жалған жұмыс істеуге ие болса да, құпия құжат белгіленбеген болса, ол желі периметрін қиып кете алмайды. Жақсы DLP жүйелерінде екі тексеру әдісі де үйлеседі. Көбінесе DLP жүйесі бірнеше модульден тұрады. Бірінші-желі периметрінің шекарасын кесіп өтуге

тырысатын трафикті бақылауға арналған желілік деңгей модулі. Желілік модуль прокси-серверлерге және электрондық пошта серверлеріне орнатылады, сондай-ақ жеке сервер түрінде орнатылуы мүмкін. Екінші – Бұл USB-жинақтағыштарға, CD-дискілерге және т. б. сияқты арналарды бақылайтын хост деңгейінің модульдері және сәйкесінше кәсіпорын қызметкерлерінің жұмыс станцияларына орнатылады. Алынбалы ақпарат тасығыштарына жазбаларды бақылаудан басқа, хост деңгейінің модулдері желілік күйге келтірулерде болған өзгерістерді, туннелдеу үшін арнайы бағдарламалық қамтамасыз етуді және бақылау жүйесін айналып өтудің басқа тәсілдерін орнатуды қадағалайды. DLP-жүйе осы модульдерді біріктіреді, ал орталықтандырылған басқару тағы бір мамандандырылған модульмен жүреді. DLP-жүйенің басым міндеті желі периметрі, қорғалатын ақпараттық жүйе шегінен тыс құпия белгісі бар ақпаратты таратуды болдырмау болып табылады. Алайда, ағып кету тек қасақана емес, ойдан тыс болуы мүмкін. Positive Techlogies компаниясының 2019 жылы жүргізген зерттеуі көрсеткендей, барлық ағып кетулердің 75%-ы жасырын, көбінесе компьютер қолданушыларының қателігінен, олардың ұқыпсыздығынан болады. DLP-жүйелердің екінші жоспарына кететін міндеттер:

- инциденттерді тексеру үшін хабарларды мұрағатталған түрде сақтау;
- құпия емес жағымсыз ақпаратты беруге тыйым салу (спам, қорлау, деректердің үлкен көлемі);
- қызметкердің компанияға тиесілі ресурстарды жеке мақсатта пайдалануға тыйым салу;
- бақылау қатысуын қызметкердің жұмыс орнында жұмыс уақыты;
- қызметкерлерге, оның саяси, діни наным-сенімдеріне келісім жинау.

3.2. Виртуалды Windows ортасы

Виртуалды Windows ортасы деп платформада-қожайында аппараттық қамтамасыз етуді имитациялайтын бағдарламалық-аппараттық жүйені түсінеміз. Бұл бір-бірінен қисынды оқшауланған және физикалық бір құрылғыда орындалатын есептеу ресурстарының жиынтығын ұсыну үшін жасалған. Мұндай өзара әрекеттестікте желіге қатынау, ақпаратты енгізу және шығару мүмкіндігі сервер жағындағы тиісті бағдарламалық жасақтаманы бақылайды. Қарастырылып отырған жағдайда деректер қоймасын виртуализациялауға баса назар аударылады. Виртуализация бірнеше ықтимал жолдармен қол жеткізіледі:

- компьютер желісінің көмегімен түрлі құрылғылардан файлдарға қатынауға мүмкіндік беретін таратылған файлдық жүйе құрылады;
- 17 виртуалды файлдық жүйе құрылады, ол клиенттік қосымшалардың түрлі файлдық жүйелерге біркелкі қатынауын қамтамасыз етеді. Серверлерде сақталған деректерге мөлдір қол жеткізу үшін жиі қолданылады;

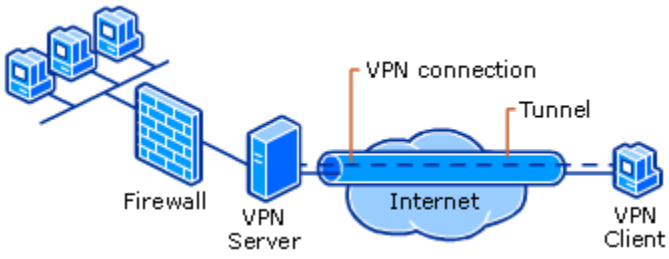
- әр түрлі физикалық тасымалдаушыларды деректердің бірыңғай логикалық массивіне біріктіру мақсатында виртуалды файлдық жүйе құрылады.

Виртуалды Windows ортасы ресурстарды виртуалдау үшін пайдаланылады, яғни физикалық торапты бірнеше бөлікке бөлу жүзеге асырылады, әрбір жеке бөлік бір нақты пайдаланушыға арналған сервер ретінде бөлінеді. Осыған орай, BYOD саясатын пайдаланатын компания пайдаланушысы Windows ортасына терминалдық сессия көмегімен қол жеткізуге болады, ол өз кезегінде жоғарыда DLP-жүйемен сипатталған сервер жағында қорғалған.

3.3. Терминалдық сессиялар

Клиенттік құрылғыны серверге қосқан кезде терминалдық сессияның көмегімен пайдаланушы тапсырмаларды орындау үшін есептеу ресурстарын алады. Ресурстар бұрын айтылғандай, клиенттердің терминалдарымен компьютерлік желі арқылы қосылған қуатты компьютер болып табылатын терминалдық серверді бөледі. Терминалдық сервермен қосылғаннан кейін, клиентке өңдеу үшін сервер жағында жергілікті сақталатын деректер, сондай-ақ принтер сияқты кейбір жергілікті құрылғылар ұсынылады. Мұндай шешімнің негізгі артықшылығы-қауіпсіздік, яғни инсайдерлік қауіп-қатерлерді төмендету.

Виртуалды Windows орталарына қосылған кезде, қызметкерлер Active Directory доменінде немесе басқа LDAP каталогында тіркелгіні авторландырғаннан кейін қол жеткізуге болады. Қол жеткізу қорғалған VPN-туннель арқылы, өз кезегінде пайдаланушының немесе құрылғының қатаң аутентификациясын қамтамасыз етеді. VPN-туннель-бұл қорғалған байланыс, туннельдің бір соңында қосылым жасағысы келетін басқа клиент үшін VPN-сервері. Байланыс басқа желінің үстіне жүреді, интернет желісі жиі пайдаланылады. Алайда, көп жағдайда коммуникациялар сенім деңгейі төмен желілердің үстінен жүргізіледі. Бұл мәселе туннель ішінде берілетін барлық деректерді шифрлеу арқылы шешіледі, бұл дегеніміз, деректер қондырма жасалған желіде шифрлеуге болмайды. Сонымен қатар, vpn технологиясында құрылған желінің сенім деңгейі базалық желілердің сенім деңгейіне байланысты емес деп айтуға болады.



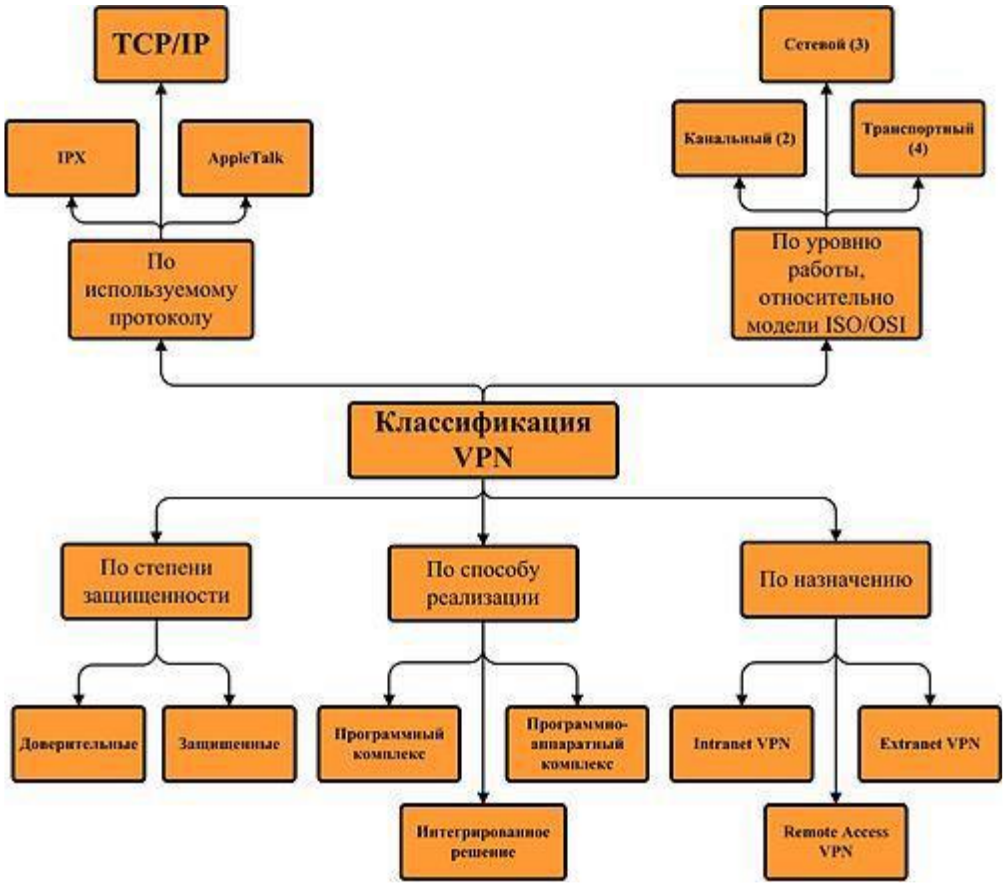
13-сурет. VPN-туннель.

Пайдаланушылардың қажеттіліктеріне байланысты, VPN желісін қосылыстардың үш түрінде құруға болады:

- нүкте-нүкте;
- нүкте-желі;
- желі-желі.

BYOD саясатын жүзеге асыру үшін қажеттіліктерге сүйене отырып, корпоративтік желілерде vpn-туннелді пайдалана отырып, нүкте-желі қосылымын пайдаланады. VPN-желілері егер қызметкер офистен тыс болса, корпоративтік деректерге қауіпсіз қатынауды қамтамасыз ете алады, өйткені туннель арқылы берілетін деректер шифрланған және провайдерлер оларды оқуға мүмкіндіктері жоқ, сонымен қатар VPN технологиясының көмегімен географиялық жағынан бөлінген бірнеше филиалдарды, бір ұйымды бірыңғай желіге қосуға болады. Көбінесе, vpn криптография әдістерін пайдалану кезінде көлік хаттамаларының өзгермейтіндігін сақтау үшін желілік (OSI деңгейлердің моделі бойынша) жоғары емес деңгейде өрістетеді. Көп жағдайларда, құру үшін VPN пайдаланылады инкапсуляция хаттамасы PPP (Point-to-Point Protocol) қандай да бір басқа да, мысалы, IP (Internet Protocol), мұндай тәсілі кезінде пайдаланылады іске асыру хаттамасы PPTP (Point-to-Point Tunneling Protocol) және іске асыру Ethernet (PPPoE) - Point-to-point protocol over Ethernet

.



14-сурет. VPN классификациясы.

VPN құрамына екі бөлік кіреді. Біріншісі бірнеше болуы мүмкін "ішкі" желіден тұрады және ол бақыланады. Екінші " сыртқы "болып табылады, ол бойынша инкапсуляцияланған байланыс болады, көбінесе Интернет желісі пайдаланылады. Қашықтағы пайдаланушыны VPN қосуы екі бөлікке қосылған кіру сервері арқылы жүзеге асырылады.

Қашықтағы пайдаланушыны қосқан кезде (немесе басқа қорғалған желімен қосылған кезде) қол жеткізу сервері сәйкестендіру процесін, содан кейін аутентификация процесін жүргізуді талап етеді. 2.6 сурет-LTE желісінің архитектурасы-LTE желісінің архитектурасы-LTE желісінің архитектурасы-LTE желісінің архитектурасы-LTE желісінің архитектурасы-LTE желісінің архитектурасы-LTE желісінің архитектурасы-LTE желісінің архитектурасы-LTE желісінің архитектурасы.

Егер VPN классификациясын жан-жақты қарастырсақ, VPN мақсаты бойынша BYOD саясатын пайдаланатын компания қызметкерінің корпоративтік ресурсы мен мобильді құрылғысы арасындағы қорғалған байланыс арнасын құру арқылы қашықтан қол жеткізуді жүзеге асыру үшін пайдаланылатыны көрініп тұр.

Осылайша, vDLP технологиясы құпия деректерге қашықтан қатынауды бақыланатын ұсыну болып табылады. Мобильді BYOD-құрылғыда Компанияның корпоративтік деректерін жергілікті сақтауға қарағанда, өз кезегінде, корпоративтік деңгейде тиісті түрде қорғалған.

Осыған орай, жоғарыда сипатталған технологияны қолдану қауіпсіздіктің негізгі үш проблемасын шешуді қамтамасыз етеді:

- деректерді қауіпсіз өңдеу-мобильді құрылғыда корпоративтік деректерді сақтау және өңдеу мүмкіндігін болдырмағанда, Компанияның құпия ақпаратын бақыланатын құрылғыдан әрі қарай тарату мәселесі шешілуде. Қашықтағы қосылымның қауіпсіз сессиясы жасалады, бұл жергілікті деректерді өңдеу үшін қолданбаларды пайдалануды болдырмайды;

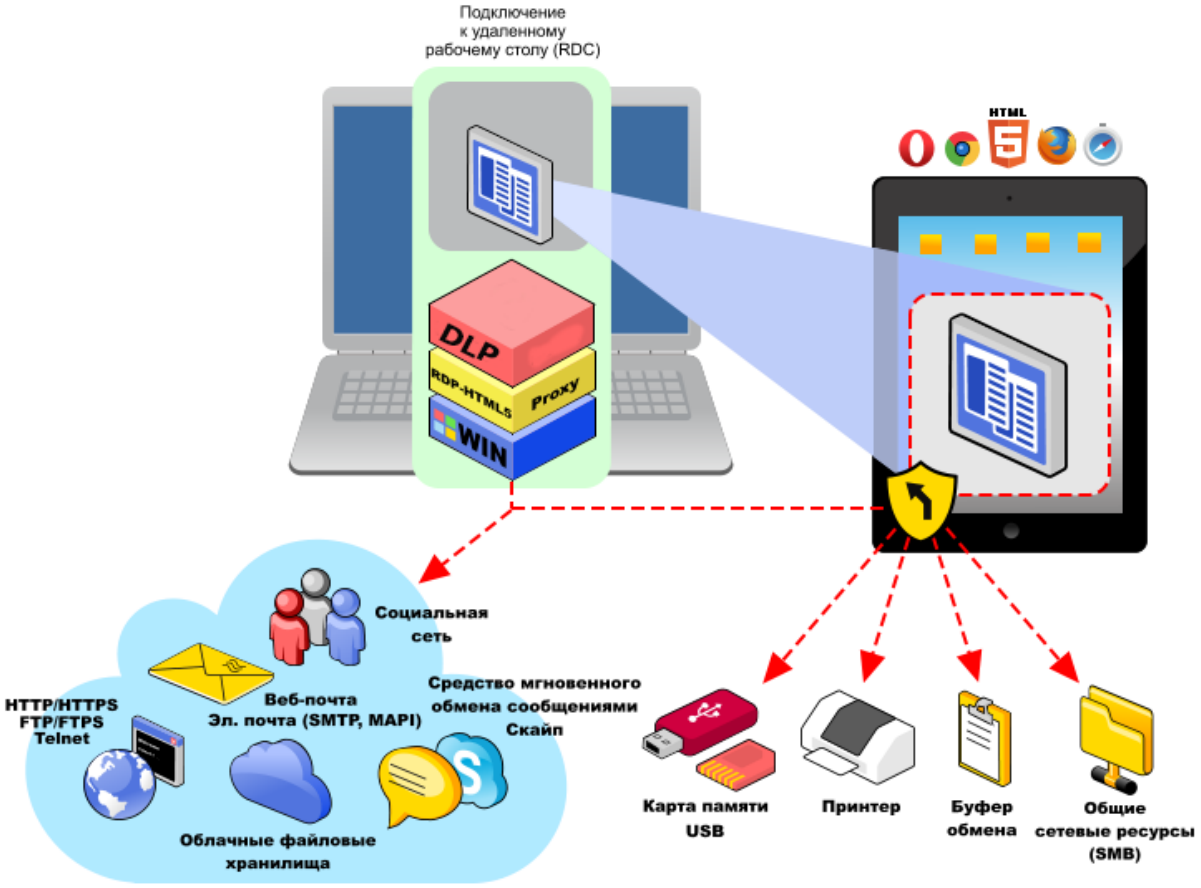
- деректерді қауіпсіз сақтау-құпия сипаты бар корпоративтік деректер компания серверінде орналасқан виртуалды ортада өңделеді. Бұл деректерді өңдеу әдісі BYOD құрылғысының жадында жергілікті деректерді сақтауды болдырмайды немесе бұл процесті бақылайды. Құжаттарды өңдеу, өзгерту, сақтау, басып шығару ұйым желісінің периметрі ішінде ғана жүргізіледі, яғни тиісті қорғау, деректердің уақытылы сақтық көшірмесін жасау жүргізіледі;

- деректер мониторингі-Virtual DLP қызметкерінің әрбір сессиясы үшін Windows виртуалды ортасында жұмыс істейтін шешім коммуникациялық арналар (электрондық пошта, вебсайттар, мессенджерлер және т.б.), жарияланған қосымшалар, баспа арнасы, қайта бағытталған дискілер және желілік файл ресурстары, сондай-ақ виртуалды хостингті бағдарламалық қамтамасыз етумен рұқсат етілген алмалы-салмалы тасығыштар арқылы өтетін файлдар мен деректердің мазмұнын сүзуді қамтамасыз етеді.

Virtual DLP шешімін пайдалану кезінде корпоративтік деректермен жұмыс істейтін барлық қосымшалар виртуалды Windows-сессия ішінде іске

қосылады, яғни шын мәнінде ұйымның "үйдегі" серверінде ғана бар. Мұндай жағдайда қызметкерлер виртуалдау серверінде жарияланған, жұмыс істеуге қажетті қосымшаларды еркін пайдалана алады, сонымен қатар ақпараттық қауіпсіздік қызметі өңделетін деректерді толық бақылауды сақтайды, өйткені сақтау BYOD құрылғысында емес, серверде жүргізіледі.

Әрине, MDM-шешімдер корпоративтік деректерді қорғаудың негізгі рөлдерінің бірін ойнай отырып, BYOD-құрылғылардың қорғалу деңгейін арттырады, алайда, MDM класының жүйелері деректердің ағуын болдырмайтынын тағы бір рет атап өткен жөн, олар DLP жүйелеріне тең емес. Сонымен қатар, бұл жүйе бір уақытта жұмыс істеуі керек, яғни жүйе бір уақытта жұмыс істеуі керек.



15-сурет. VDLP технологиясы.

Қызметкерлерге тиесілі мобильді құрылғыларды бизнес-процестерге, техникалық мәселелерге және т.б. жылдам интеграциялауды жүргізуді шешкен ұйымдарға көмек мамандандырылған DLP-жүйелер көрсетеді. Корпоративтік деректерді сақтау ережелері, оларды өңдеу, беру тәсілдері, сондай-ақ бизнес үшін аса маңызды деректерді анықтау сияқты аспектілерге ерекше назар аудару қажет.

Бұрын айтылғандай, компания қызметкерлерінің жеке пайдалануындағы және желі периметрінің ішіне кіретін мобильді құрылғылар саны одан да көп болады. Мұндай құрылғылар Смартфондар, планшеттер, USB

жинақтағыштар, MP3-плеерлер, түрлі камералар болып табылады. Ал бұлтты сақтау сервистерін жылдам дамыту, әлеуметтік желілерді, әртүрлі желілік қосымшаларды дамыту және санамаланғандардың жалпы қол жетімділігі жағдайында құпия деректердің бақыланбайтын жылыстауының пайда болуына қосымша қауіп туындайды. Бұл мәселені шешуге резиденттік DLP жүйелері көмектеседі.

Резиденттік қорғау антивирустық қорғау рөлін атқаратын бағдарламалық қамтамасыз ету компоненті болып табылады. Компонент жедел жадыда орналастырылады және нақты уақыт режимінде пайдаланушы, операциялық жүйе немесе өзге де бағдарламалар өзара әрекеттесетін деректер мен файлдарды үздіксіз сканерлеу жүзеге асырады. Резиденттік қорғау-бұл фондық режимде, яғни пайдаланушы үшін көрінбейді. Сонымен қатар, резиденттік қорғаныс кез келген вирусқа қарсы бағдарламалық қамтамасыз етудің басты компоненті болып табылады, оның негізгі міндеті компьютерді жұқтыруға жол бермеу болып табылады.

Құпия деректерді тиісті түрде қорғауды қамтамасыз ету үшін әртүрлі деңгейде және әртүрлі тәсілдермен бақылауды жүзеге асыру қажет (жоғарыда деректер контекстінің талдауы және деректер мен файлдардың мазмұнын талдау сипатталғандай). Жоғарыда айтылғандарды негізге ала отырып, компанияда ақпараттық қауіпсіздік мәселелерімен айналысатын мамандар пайдаланушылар мен топтар үшін, BYOD-құрылғыларды пайдаланатын қызметкерлердің өнімділігі мен нәтижесінде компания беделінің төмендеуі, мәмілелердің бұзылуы, айыппұлдар мен өзге де Санкциялар болуы мүмкін құпия деректерді жоғалту тәуекелі арасында сауатты қол жеткізу құқығын белгілей отырып, балансты табуға тиіс.

Әрине, пайдаланушылар деректерге әрдайым жеткілікті қол жеткізе алмайтынын, арнаның өткізу қабілетінің жетіспеушілігіне немесе кеңседен тыс (мысалы, ұшақта, үшінші әлем елдерінде және т.б.) желілік қосылыстың жоқтығына тап болатынын, демек, корпоративтік деректерді дербес мобильді құрылғыларда жергілікті сақтауға мүмкіндігі болуы тиіс. Және бұл ақталған жағдайда мүмкін болады. Дегенмен, көптеген ұйымдар үшін Virtual DLP моделі шектеулі қолжетімділіктің деректерін жоғалтудың нақты тәуекелінен гөрі ымыралы болады.

3.4. BYOD стратегиясы қауіпсіздік формуласы

Келесі оңайлатылған формула BYOD қауіпсіздік стратегиясын қамтиды:

BYOD = "MDM" + "App" + "VPN" + "VM" + "DLP", онда:

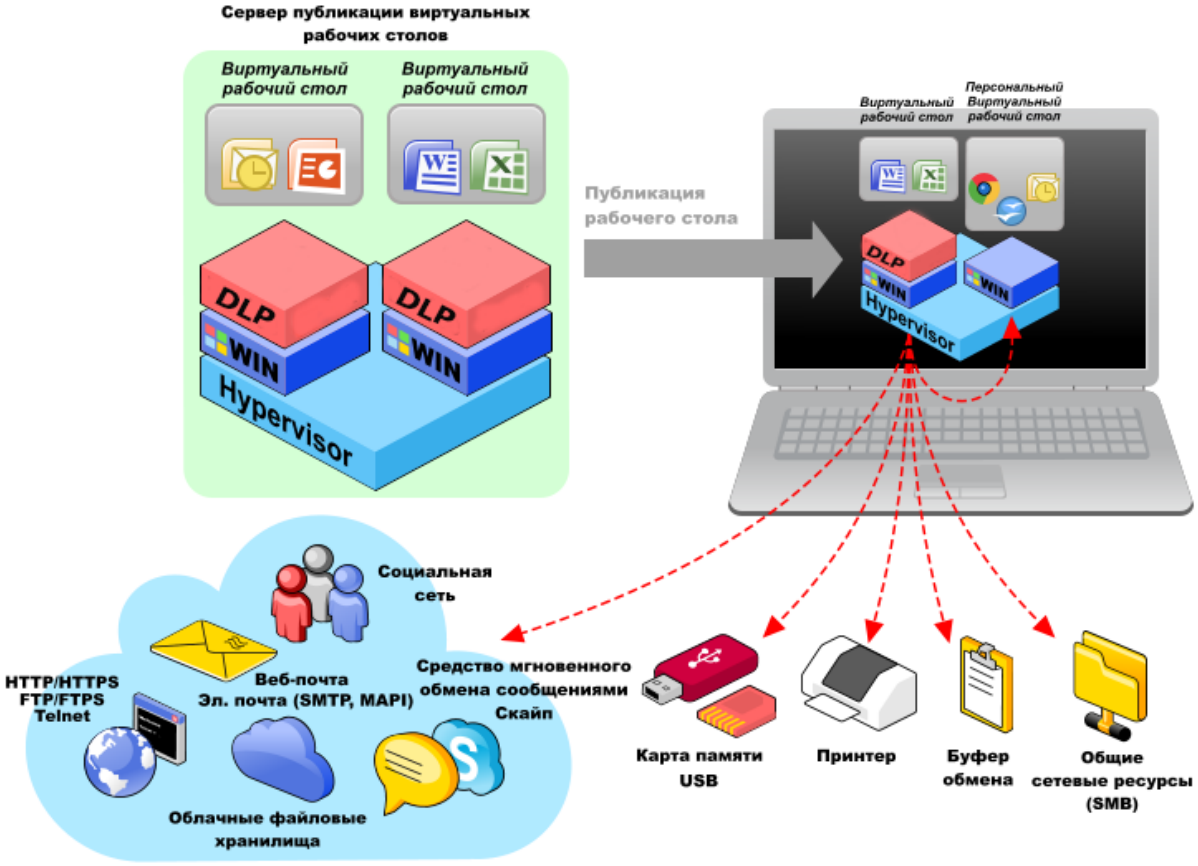
"MDM" - құрылғыдағы жергілікті қосымшаларды бақылауға, деректерді қашықтан жоюға, құрылғының сенімді құпия қорғанысын қамтамасыз етуге және деректерді шифрлауға және т. б. арналған жүйе;

"App" - ұялы құрылғыны интернет арқылы ұйым Қосымшаларының виртуалды хостингіне қашықтан қосуға арналған қосымша (мысалы, Citrix Receiver).

"VPN" - SSL криптографиялық хаттамасымен қорғалған ұйымның виртуалды жеке желісіне (Virtual Private Network) қосылу, жарияланған қосымшалармен, оның ішінде пайдаланушыларды қосымша аутентификациялау үшін пайдаланылатын.

"VM" -пайдаланушыларға жұмыс ортасын ұсынатын Citrix / WTS / MS RDx / т. б. виртуалдау құралдары негізіндегі Windows-жүйесін виртуалды іске асыру.

"DLP" -BYOD-құрылғысынан деректердің ағуын болдырмау үшін осы виртуалды ортада қол жетімді деректерді беру арналарын (электрондық пошта, вебсайттар, мессенджерлер, басып шығару арнасы, жергілікті USB-құрылғылар виртуалды ортаға қайта бағытталған) бақылауды қамтамасыз ететін Windows виртуалды Жұмыс ортасына біріктірілген деректер ағуын болдырмау жүйесі.



16-сурет. BYOD қауіпсіздік схемасы.

Экономиканың барлық салаларының компаниялары мен ұйымдары корпоративтік, құпия және дербес деректердің сақталуын қамтамасыз етуге, оларды брандмауэрмен қорғалған периметрден кейін және авторизациялаудың күрделі әдістерімен қамтамасыз етуге күш пен құралдардың массасын жұмсайды. Бірақ, өкінішке орай, объективті шындық периметрді қорғау жеткіліксіз және мұқият қорғалатын деректер әлі де саусақтар арқылы ағады. Қызметкерлердің жұмыс орындарының ұтқырлығы

деңгейінің қарқынды өсуі барлық үдемелі консьюмеризациялаумен (түрлі дербес құрылғыларды белсенді қолданумен) ұштастыра отырып, деректердің жылыстауына жаңа қауіп төндіреді, олармен ұйымдар бүгінгі күні белсенді күресуге мәжбүр.

Мобильді құрылғылар көбінесе қорғалған офистік желілерден тыс пайдаланылғандықтан, периметр қауіпсіздігінің дәстүрлі компоненттері мобильді құрылғылардан коммуникацияларды тиісті бақылауды және мониторингілеуді қамтамасыз ете алмайды. Бұдан басқа, ұялы құрылғылардың физикалық жоғалу немесе ұрлану қаупі туралы есте сақтау қажет.

BYOD тиімді стратегиясы құрылғыларда қажет болған жағдайда деректерді басқару, бақылау және жою ғана емес, сонымен қатар мобильді құрылғылардан деректердің ағуын болдырмау болып табылады. Бұл ретте деректерді бақылаудың контекстік және контенттік әдістерін қолдану керек.

DLP-технологиялардың негіздерін айқындайтын іргелі қағидаттардың арқасында дербес мобильді құрылғыларды кәсіпорынның бизнес-процестеріне жылдам интеграциялау міндетін шешетін ұйымдар үшін деректердің жылыстауын болдырмау технологиялары (DLP) өте пайдалы және тиімді болады. Бұл жерде ұйым үшін қиын деректер мен оларға қол жеткізу саясаттарын нақты бөлу, сақтау, тасымалдау және беру саясаттарын анықтау, сондай – ақ деректерді пайдалану-бұл жиынтығында файлдар мен деректерді ұйымдастыру үшін құнды қорғаудың тұтас технологиясын құрайды.

3.5. Қорытындылар

Жүргізілген талдау барысында келесі қорытындылар жасалды:

1. MDM класындағы шешімдердің кемшіліктерін талдау ұялы құрылғыларды басқару жүйесі кешенді сипатқа ие болатын кең қорғаныс үлесінің бөлігі болуы мүмкін деп айтуға мүмкіндік береді. Жоғарыда қарастырылған жүйені деректерді шифрлау және басқару, жалпы мобильді құрылғыларды бақылау сияқты міндеттерді шешу үшін соңғы қорғаныс шарасы ретінде қолдану қажет. Тек осы жағдайда ғана мобильді контентті басқару жүйесінің жұмысы тиімді болады.

2. Virtual DLP әдісі корпоративтік деректерге қол жеткізу үшін пайдаланылатын мобильді құрылғылардың қауіпсіздігін қамтамасыз ету саласында неғұрлым тиімді болып табылады. Әдістің мәні-пайдаланушы өзінің жеке мобильді құрылғысынан Компанияның корпоративтік деректеріне қашықтағы қосылу арқылы қол жеткізе алады. BYOD-құрылғы виртуалды Windows орталарына терминалдық сессиялар арқылы қашықтан қосылады. Windows-орталар, өз кезегінде, DLP-жүйемен қорғалады, ол хостада жұмыс істейді, соның арқасында бақыланбайтын деректердің кемуін болдырмайды.

3. BYOD-құрылғыларды кешенді қорғау стратегиясы: қауіпсіздік BYOD = "MDM" + "App" + "VPN" + "VM" + "DLP". BYOD тиімді стратегиясы құрылғыларда қажет болған жағдайда деректерді басқару, бақылау және жою

ғана емес, сонымен қатар мобильді құрылғылардан деректердің ағуын болдырмау болып табылады. Бұл ретте деректерді бақылаудың контекстік және контенттік әдістерін қолдану керек.

ҚОРЫТЫНДЫ

Бітіру біліктілік жұмысын орындау барысында алынған басты нәтиже – BYOD саясатының қауіпсіздік формуласын жақсарту үшін скриншоттарды блоктаудың әзірленген бағдарламасы.

Алға қойылған міндеттерді шешу барысында:

1. BYOD ақпаратының қауіпсіздігі саласында жүргізілетін жұмыстардың өзектілігі анықталды, себебі көрсетілген стратегияны пайдаланудың жылдам өсуі ақпараттың жылыстауы санының артуына алып келеді, ал ұялы құрылғыларды қорғау үшін ұсынылатын шешімдер олардың өндірушілері көрсеткеніндей тиімді емес.

2. Mobile Device Management (MDM) шешімдер класы қарастырылды. Алайда, анықталды, бұл қарамастан, өзінің барлық қадір-қасиетін жүйесі бар елеулі кемшілігі – бұл басқарылатын жою болған кезде ғана құрылғы желі жұмыс істейді. Сонымен қатар, рұқсат шектелген құпия деректер BYOD құрылғыларында қауіпсіз құрыла алмайды және сақталады. Сонымен қатар, MDM-жүйелер DLP-жүйелеріне тең деп айтуға болмайды, себебі MDM әртүрлі жағдайларда деректерді талдау функцияларына ие емес және мобильді девайсқа сенімді MDM қол жетімділігіне байланысты, пайдаланушының контексті бойынша, ақпараттың мазмұны бойынша қосылатын сыртқы ақпарат тасығыштарын сүзу жоқ.

3. Зерттеу жүргізілді, оның нәтижелері қазіргі бар BYOD қауіпсіздік формулалары құпия деректерді сақтау үшін жеткіліксіз екенін анық түсінуге мүмкіндік береді. Қолданыстағы тыңшылық-бағдарламаларға талдау жүргізілді, олар құрылғының пайдаланушысы үшін жиі байқаусыз және вирусқа қарсы ақпаратты ұрлайды және қаскүнемге жібереді. Зерттеу барысында аса күрделі бағдарламаны орнату және тексеру жүргізілді.

4. BYOD тиімді стратегиясы анықталды, ол тек құрылғылардағы деректерді басқару, қадағалау және жою ғана емес, қажет болған жағдайда – сонымен қатар мобильді құрылғылардан деректердің ағуын болдырмау болып табылады. Бұл ретте бақылаушылардың контекстік және контенттік әдістерін пайдалану керек. BYOD қауіпсіздік формуласы шешімдер жиынтығы болып табылады: қауіпсіздік BYOD = "MDM" + "App" + "VPN" + "VM" + "DLP".

ҚОЛДАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1 Hayes, B. Bring Your Own Device (BYOD) to Work / B. Hayes. – Лондон: Newnes, 2013. – 463 с.

2 Мобильді технологияларды пайдалану ресейлік бизнестің ажырамас бөлігі болып табылады : Citrix зерттеуі. – сайттағы электронды нұсқасы https://www.citrix.com/news/announcements/oct-2016/the-reluts-of-mobility-survey-held-in-russia-ru.html

3 Pierer, M. Mobile Device Management: Mobility Evaluation in Small and Medium-Sized Enterprises / M. Pierer. – Вена: Wiesbadenб 2014. – 217 с.

4 Rains Tim. Trust in Computing Survey, Part I: Consumerization of IT Goes Mainstream / T. Rains. – сайттағы электронды нұсқасы https://blogs.microsoft.com/microsoftsecure/2013/07/10/trust-in-computing-survey-part-i-consumerization-of-it-goes-mainstream

5 BYOD қауіпсіздігі туралы 5 аңыздар /- сайттағы электронды нұсқасы http://www.devicelock.com/ru/articles/detail.html?ID=2558

6 MDM Mobile Security Solutions – сайттағы электронды нұсқасы https://www.mobileiron.com/en/solutions/mobile-security

7 Андрианов, В.В. Обеспечение информационной безопасности бизнеса: практическая энциклопедия / В.В. Андрианов, В.Б. Голованов. – М.: Литрес, 2013. – 450 с.

8 Чекмарев А.Н. Microsoft Windows 7. Руководство администратора / А.Н. Чекмарев. – Санкт-Петербург: BHV-СПб, 2010. – 896 с.

9 Борисов М. А. Основы программно-аппаратной защиты информации / М.А. Борисов, И. В. Заводцев, И. В. Чижов. – М.: УРСС: Либроком, 370 с.

10 Вульф М. М. Как защитить компьютер от вирусов / М. М. Вульф, Н. Т. Разумовский, Р. Г. Прокди. – Санкт-Петербург: Наука и техника, 190 с.

11 Лебедев А. Защита компьютера от вирусов, хакеров и сбоев / Алексей Лебедев. – М.: Питер, 2013. – 157 с.

12 Левин М. Библия хакера 2. Книга 1 / М. Левин. – М.: Майор, 2003. – 638 с.

13 Матвеев М. Д. Администрирование Windows 7 / М. Д. Матвеев, Р. Г. Пронди и др. – Санкт-Петербург: Наука и техника, 2013. – 396 с.

14 Observer бағдарламасы туралы / - сайттағы электронды нұсқасы http://www.observer.ooo/faq

Қосымша А

Атауы	Мобильді құрылғылармен қосымшаларды басқару	Ақпаратты қорғау	Соңғы нүктенің масштабталуы	Жылдам жайылу	Бағасы тг/ай
Microsoft Intune	+	+	+	-	3191
IBM MaaS360	+	+	+	-	1517
Cisco Meraki	+	+	+	+	2836
VMware Airwatch	+	+	+	+	4130
MobileIron EMM	-	+	+	+	2653
SAP MobileSecure	+	+	+	+	-
TrendMicro MobileSecure	+	+	-	-	11370
XenMobile	+	+	-	-	11182
Manage Engine Mobile Device Manager Plus	+	+	-	+	18792
BlackBerry Enterprise Mobile Suite	+	+	-	+	-
Jamf Pro	+	+	+	+	2653
Avalanche Mobility Center	-	+	-	-	1579
Kasey EMM	-	+	-	+	1137
Absolute Manage MDM	+	+	-	-	1921
SOTI MobiControl	+	+	+	+	3960
Tangoe Managed Mobility Services	-	+	-	-	1708
Sure MDM	+	+	-	-	-
MobiLock Pro	+	+	-	-	6822