ОӘЖ 004.056.53

ҚАУІПСІЗ ВИДЕОКОНФЕРЕНЦИЯЛАР ӨТКІЗУ ӘДІСТЕМЕСІН ӘЗІРЛЕУ

Дәндібай Аманбол Әділдинұлы
amanboldandibay@gmail.com
Л.Н. Гумилев атындағы Еуразия Ұлттық Университеті, Ақпараттық технологиялар факультеті, 7М06306 – Ақпараттық қауіпсіздік жүйелері мамандығының 1 курс магистранты, Нұр-Сұлтан қ., Қазақстан
Ғылыми жетекшісі – Бекманова Гульмира Тылеубердиевна

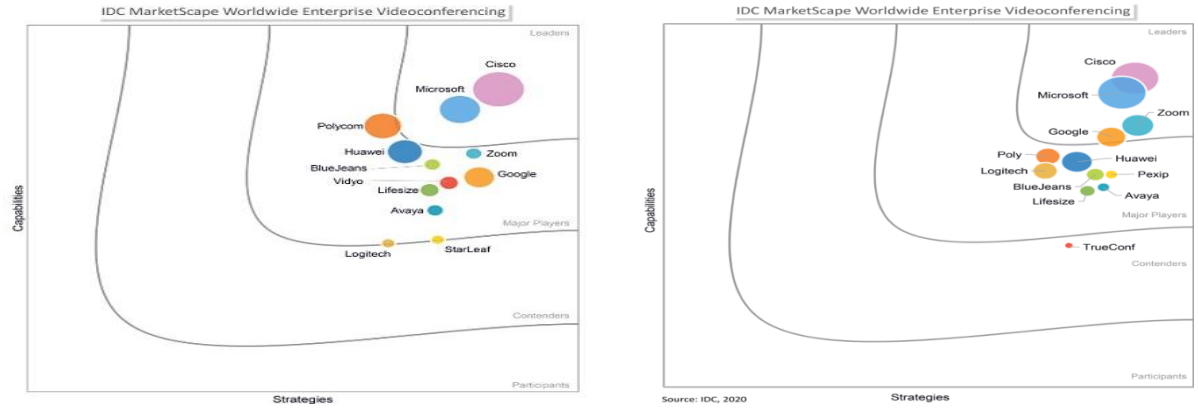
Кіріспе. Видеоконференция – компьютерлік технологиялардың ақпараттық және бағдарламалық құралдарын қолдана отырып, дәл қазіргі уақыт режимінде бейне ақпаратты екі жақты беруді, өңдеуді, түрлендіруді және қашықтықтан видео-ақпаратты ұсынуды қамтамасыз ететін ақпараттық технологияның саласы [1].

Қазіргі таңда қызметтік жиналыстар, лекциялар, семинарлар, тіпті емтихандар мен сынақтар, кез-келген топтық жиналыстар, көбінесе бір-бірінен едәуір қашықтықта орналасқан бірнеше абоненттермен видео байланыс қызметін ұсынатын, видеоконференция сервистері – арнайы бағдарламалар мен қосымшалар арқылы жүзеге асырылады. Кейбір видеоконференция қызметтері файлдарды абоненттер арасында бір-бірімен бөлісуге

мүмкіндік береді. Сұраныстың жоғары болуы жаңа ұсыныстарды тудырады, сондықтан нарықтағы бар қосымшаларға жаңа функциялар мен қызметтерді енгізуіне алып келді.

Мәселен қазір жиі қолданылатын видеоконференция қосымшалары: Zoom, Microsoft Teams, Cisco Webex Meetings және т.б..

Соңғы жылы әлемде болып жатқан өзгерістер видеоконференция қосымшаларының үлкен өзгерістеріне алып келді. Әртүрлі компаниялардың зерттеулерінің арқасында аналитика нарықтың тек дамуын көрсетеді. Мысалға IDC зерттеу компаниясының 2018 және 2020 жылғы шілде айындағы зерттеулері бойынша видеконференция қосымшаларын өндіруші компаниялардың нарықта үлкен қолданысқа ие болғандығы байқалады [2].



а) ә)

Сурет 1 Дүниежүзілік корпоративтік видеоконференция байланысы өндірушілерін бағалау (IDC MarketScape бойынша): а)2018 жыл; ә)2020 жыл [2].

Әр қосымшаның өзінің артықшылығы мен кемшіліктері бар, Интернет желісіндегі кез-келген сервистер сияқты видеоконференцияны қолданудың белгілі-бір өзіндік қауіптері бар және уақыт өте келе олардың осалдылықтары да анықтала бастайды.

Ғаламтордағы қаскөйлердің негізгі мақсаты қолданушылардың жеке бас ақпараттарына немесе ақшалай қаражаттарына қол жеткізу. Өздерінің қалағанына қол жеткізу үшін олар қолданушыларды алдаудың және зиянкес бағдарламалық қамтамаларды таратудың жаңа тәсілдерін ойлап табады. Видеоконференция құрылғыларының кеңінен таралуы қаскөйлердің оларға деген назарын ерекше аудартып, 2020 жылғы сәуірде «Лаборатория Касперского» компаниясының мамандары мыңнан астам зиянкес кодтар мен жағымсыз қамтамасыздары бар файлдарды анықтады [3]. Ұрланған ақпараттар бопсалау үшін немесе социалды инженерия арқылы алдыңғы уақытта шабуылдар жасауға қолданылуы мүмкін. Ең белгілі жағдайларға ашық қолданысқа дәрігерлермен кездесулер, психотерапия сеанстарының жазбалары және қаржылық есептер қарастырылған, компаниялардың жиналыстарының жариялануы. Осы себепті қолданушылар үшін қауіпсіз видеоконференцияларды өткізу әдістемесін әзірлеу қазіргі уақыттағы маңызды сұрақтардың бірі болып отыр.

Әдістемені әзірлеу үшін ақпараттың қандай жолдармен таралып кетуі мүмкіндігін қарастыру қажет:

- Жалған қосымшалар. Мұндай қосымшалар ресми қосымшаларға қатты ұқсас болып келеді, тіпті олардың есімдері мен интерфейстерін көшіріп алады. Бірақ, айтылған функциялардың орнына, олар құрастырушыларының талаптарын ғана қанағаттандырады. Қосымшаға тіркелген уақытта жеке бас ақпараттар шабуылдаушыға барып түседі.

- Видеоконференция қосымшаларынан жеке ақпараттардың таралып кетуі. Ақпараттардың таралып кетуінің себептерінің бірі, бұрыннан бар осалдылықтар арқылы, шабуылдаушыларға жеке кабинетке санкцияланбаған қолжетімділік және конференцияларды

жазып алуға мүмкіндік береді. Тағы бір себебі, жеке кабинетке өтетін құпия сөздің басқа да сервистерде қолданылуы.

- Байланыс уақытында немесе одан кейін жеке ақпараттардың таралып кетуі. Бұл жағдайда да бірнеше себептерді атап өтуге болады. Біріншіден, қолданушының экранда қажеттен тыс ақпараттарын көрсетуі. Мысалғы, демонстрация уақытында қолданушының жеке құжаттарын, браузердің іздеу сұрауларын немесе файл атауларының өзін көрсетуі. Екіншіден, конференция қатысушыларын қадағалаудың жоқтығы. Конференция администраторы, өзге таныс емес немесе бөгде адамдардың кіріп кетуін болдырмау үшін, байланысқа қосылып отырған қатысушыларды тексеріп отыруы қажет. Үшіншіден, конференцияны жазу және ақпарат алмасу кезіндегі шифрлау алгоритмінің осалдылығы немесе мүлдем болмауы [4].

Ақпараттың таралып кетуі мүмкін жолдарына байланысты, әдістемеде қолданушыларға видеконференция құралдарын пайдалану барысында ұстануы қажет ұсынымдарды көрсету негізгі мақсат болып табылады. Олар:

1. Қосымшаларды тек сенімді ақпарат көздерінен жүктеу қажет: әзірлеуші сайтынан немесе ресми қолданба сатушыларынан.

2. Қолданушының жеке кабинеті сенімді әрі қайталанбайтын құпия сөзбен қорғалуы қажет, ең сенімдісі мультифакторлы аутентификациямен қосылу.

3. Қосымшаны орнатқаннан кейін, құрылғыда сақталған жеке ақпаратқа қолжетімділікті шектеген дұрыс: файлдарға, телефон номерлеріне, фото, бейнежазбаларға және т.б.

4. Құпиялық баптауларын тексеру. Видеоконференция уақытында басқа қолданушыларға қандай ақпараттар қолжетімді болатынын, байланыс аяқталғаннан кейін жазбалар қалуы мүмкіндігін түсіну қажет.

5. Бөгде қолданушылардың тіркелуін болдырмау мақсатында, видеоконференция сеанстары құпия сөзбен қорғалған болуы қажет.

6. Ашық қолданыста видеоконференция сеанстарына қосылу үшін қажет сілтемелер мен құпия сөздерін жарияламалау.

7. Видеоконференция сілтемесі сенімді ақпарат көзінен алынғандығын тексеру. Таныс емес жіберушіден келген сілтемелерді қолданбау.

8. Қатысушыларды «күту бөлмесінен» тек администратордың келісімімен негізгі чатқа қосуды баптау.

9. Егер байланыс сеансы кезінде құпия ақпарат немесе файлдармен алмасу қажет болса, видеоконференция қосымшасының сенімділігін тексеру қажет. Көптеген видеоконференция қосымшалары ақпараттарды шифрлауда end-to-end функциясын қолданатындығы айтылады, бірақ тексерулер кезінде бұл шынайы болмай, компания серверлерінде дешифрланады. Сонымен қоса, баптауларда шифрлау функциясы әдетте өшіріліп тұруы мүмкін. Одан кейін, кейбір сервистерде шифрлау тек хат алмасу мен файлдар алмасу кезінде ғана қарастырылып, аудио- және бейнехабарласу кезінде қарастырылмауы мүмкін.

10. Видеобайланыс сеансы алдында құрылғыдағы камера объективінің бөлісуді қажет етпейтін артық заттарды қамтымуын тексеру. Ең дұрысы, көп видеоконференция сервистері ұсынатын фонды алмастыру немесе бұлыңғырлау функцияларын қолдану.

11. Қызметтік жиналыс немесе оқу барысында, басқа қолданушы сөйлеп жатқанда, микрофон мен бейнекамераны өшіріп тастаған дұрыс.

12. Конференция аяқталғаннан кейін одан міндетті түрде шығып кету қажет.

13. Құрылғының операциондық жүйесін және қосымшаны жаңартып отыру, осалдылықтарды пайдаланып кетудің тәуелділігін төмендетеді.

14. Актуалды базасы бар антивирус қосымшасын қолдану. Қолданушылардан келген файлдарды тексеруден өткізгеннен кейін ғана пайдалану.

Әдістемелерге қойылатын талаптардың бірі оның өзектілігі, осыған байланысты нарықты әр уақытта зерттеу және анализдеу арқылы әдістемелерді жаңартып отыру қажет.

Қортынды. Видеоконференция қосымшалары қазір өте қарқынды дамып тек бизнес үшін жаңа мүмкіндіктер жасап қана қоймай, сонымен бірге қашықтықтан оқыту мен корпоративті тренингтерді өткізуді жеңілдетіп отыр. Видеоконференция байланыс жүйелерінің болашақта дамуы қазіргі уақытта бар тенденциялардың жалғасуын болжайды: бұлтты сервистерге сұраныстың басым болуы, жоғары сапалы бейнелерді пайдалану, басқа да ақпараттық жүйелермен және сервистермен интеграциялану, VaaS (Video as a Service) қызметтеріне сұраныстың өсуі. Бұның барлығы қауіпсіздікке де жоғары талап қояды. Сол себепті қауіпсіз видеоконференцияларды өткізу әдістемесін әзірлеп, қоданушыларға алдын-ала таныстыру тиімді шешімдердің бірі болады.

Қолданылған әдебиеттер тізімі

1. Видеоконференция [Электрондық ресурс] / Wikipedia, 2021. – Қол жеткізу режимі: https://ru.wikipedia.org/ . – Қол жеткізу уақыты: 31.03.21
2. IDC MarketScape [Электрондық ресурс] / IDC, 2018. – Қол жеткізу режимі: https://www.idc.com/. – Қол жеткізу уақыты: 31.03.21
3. Известные проблемы в приложениях для видеоконференций [Электрондық ресурс] / АО «Лаборатория Касперского», 2021. – Қол жеткізу режимі: https://www.kaspersky.ru/blog/videoconference-software-security/28287/ . – Қол жеткізу уақыты: 31.03.21
4. Костиков А.Н. Видеоконференцсвязь: проблемы и пути их решения: Электронное научное издание «Высшее образование в России» 2009, №8, С.104 – 108