ҒТАМР 28.23.15
ӘОЖ 004.056.53

С.Е. Адилькешев, В.Г. Носов, А.М. Утеев, Ж.И. Титова

Карагандинский индустриальный университет, г. Темиртау
(E-mail: v.nossov@tttu.edu.kz)

DLP жүйелерінің жедел хабаршыларда деректердің ағып кетуін болдырмаудағы тиімділігі

Қазіргі цифрлық дәуірде жедел хабаршылар (мессенджерлер) күнделікті коммуникацияның ажырамас бөлігіне айналды. Алайда, бұл платформалар арқылы құпия деректердің ағып кету қаупі де артуда. Бұл зерттеу деректердің жоғалуын болдырмау жүйелерінің (Data Loss Prevention, DLP) жедел хабаршылар арқылы ақпараттың рұқсатсыз таралуын азайтудағы тиімділігін бағалауға бағытталған. Зерттеу барысында DLP технологияларының әртүрлі түрлері, олардың функционалдық мүмкіндіктері және нақты қолдану жағдайлары талданды. Нәтижелер DLP жүйелерінің тиімділігі олардың конфигурациясына, пайдаланушылардың сауаттылығына және мессенджерлердің шифрлау деңгейіне байланысты екенін көрсетті.

Түйін сөздер: DLP жүйелері, жедел хабаршылар, деректердің ағып кетуі, ақпарат қауіпсіздігі, шифрлау, киберқауіпсіздік.

Кіріспе

Жедел хабаршылар (WhatsApp, Telegram, Slack, Signal және т.б.) қазіргі заманда жеке және корпоративтік коммуникацияның негізгі құралдарына айналды. Бұл платформалардың қолжетімділігі, жылдамдығы және пайдаланудың қарапайымдылығы оларды күнделікті өмірдің ажырамас бөлігі етті. Мысалы, WhatsApp әлем бойынша миллиардтан астам қолданушысы бар платформа ретінде жеке хабарламалардан бастап іскерлік топтардағы коммуникацияға дейін қолданылады. Telegram өзінің жоғары қауіпсіздік деңгейімен танымал болса, Slack корпоративтік ортадағы командалық жұмысты жеңілдетеді. Бұл платформалардың ыңғайлылығы ақпарат алмасуды тездеткенімен, құпия деректердің ағып кету қаупін де арттырып отыр.

Қазіргі уақытта компаниялардың көпшілігі құпия ақпаратты – мысалы, клиенттердің жеке деректерін, қаржылық есептерді немесе ішкі стратегиялық жоспарларды – қорғауға тырысады. Алайда, қызметкерлердің мессенджерлер арқылы осындай ақпаратты бөлісуі немесе байқаусызда сыртқа жіберуі сияқты жағдайлар жиі кездеседі. Мысалы, қызметкер жеке құрылғысындағы WhatsApp арқылы құпия құжатты әріптесіне жіберуі мүмкін, бірақ бұл процесс компанияның қауіпсіздік саясатынан тыс қалады. Сонымен қатар, сыртқы тараптардың – хакерлердің немесе бәсекелестердің – мессенджерлердегі деректерді ұстап алу әрекеттері де өсуде. Бұл жағдайлар киберқауіпсіздік саласындағы мамандарды деректердің рұқсатсыз таралуын болдырмаудың тиімді әдістерін іздеуге итермеледі. Осыған байланысты, DLP (Data Loss Prevention – Деректердің Жоғалуын Болдырмау) жүйелері ақпарат қауіпсіздігін қамтамасыз етудің маңызды құралы ретінде қолданылады.

DLP жүйелерінің негізгі мақсаты – құпия деректердің рұқсатсыз таралуын анықтау және оның алдын алу. Бұл технологиялар желідегі трафикті бақылау, терминалдық құрылғылардағы деректерді қадағалау және бұлттық ортадағы ақпаратты қорғау сияқты әртүрлі деңгейлерде жұмыс істейді. Жедел хабаршылар контексінде DLP жүйелері хабарламалардың мазмұнын талдап, құпия ақпараттың (мысалы, банк картасы нөмірлері, жеке сәйкестендіру кодтары немесе құпия сөздер) сыртқа шығуын блоктай алады. Бұл зерттеу DLP жүйелерінің осы платформалардағы деректер қауіпсіздігін қамтамасыз етудегі тиімділігін және олардың шектеулерін анықтауға бағытталған.

Жедел хабаршылардың танымалдығының артуымен бірге олардың қауіпсіздік мәселелері де күрделене түсуде. Мысалы, Telegram және Signal сияқты платформалар соңғы нүктеден нүктеге шифрлауды (end-to-end encryption) қолданады, бұл хабарламаларды тек жіберуші мен алушы ғана оқи алатынын білдіреді. Бұл қауіпсіздікті арттырғанымен, DLP жүйелері үшін қиындық тудырады, себебі шифрланған деректерді талдау мүмкін емес. Ал WhatsApp сияқты платформалар шифрлауды

қолданғанымен, олардың серверлері арқылы деректерді өңдеу процесі DLP құралдарына белгілі бір деңгейде қолжетімділік береді. Slack сияқты корпоративтік мессенджерлер болса, әкімшілік бақылаудың жоғары деңгейін ұсынады, бұл DLP интеграциясын жеңілдетеді.

DLP жүйелерінің тиімділігі олардың дұрыс конфигурациялануына және қолданушылардың сауаттылығына байланысты. Мысалы, егер компания қызметкерлері мессенджерлерді жеке құрылғыларында қолданса, DLP құралдарының бақылау мүмкіндігі шектеледі. Сондай-ақ, кейбір жағдайларда қызметкерлер қауіпсіздік саясатын әдейі немесе байқаусызда бұзуы мүмкін. Осыған байланысты, DLP технологиялары тек техникалық шешім ғана емес, сонымен қатар ұйымдық шаралармен – қызметкерлерді оқытумен және саясатты қатаң сақтаумен – толықтырылуы қажет.

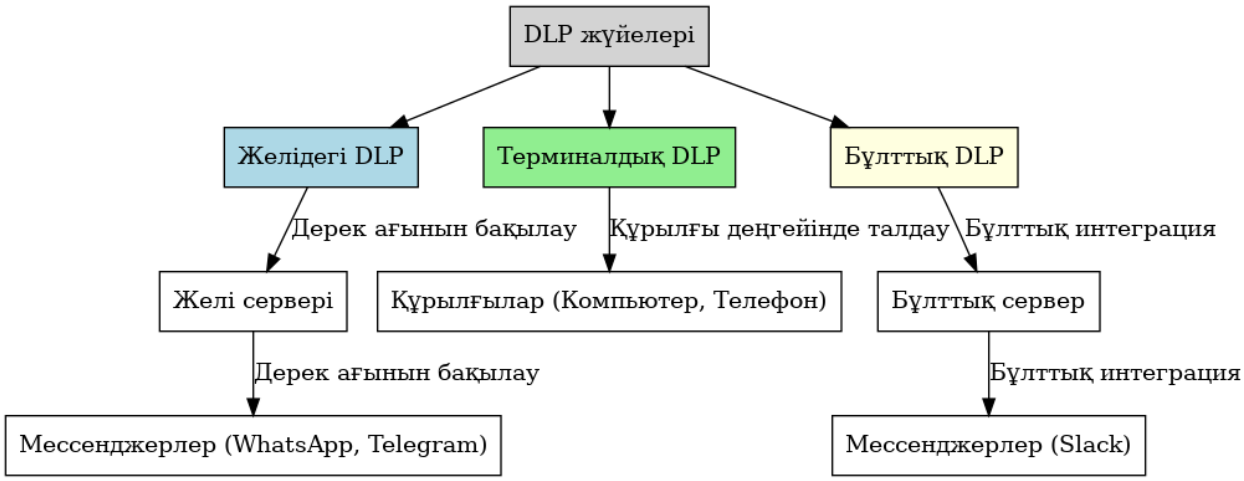
Бұл зерттеу мессенджерлердегі деректер қауіпсіздігін қамтамасыз етудегі DLP жүйелерінің рөлін жан-жақты талдауға арналған. Зерттеу барысында теориялық және практикалық әдістер қолданылып, нақты қолдану сценарийлері зерттеледі. Зерттеудің мақсаты – DLP технологияларының қазіргі мүмкіндіктерін бағалау және олардың бола municipalse тиімділігін арттыру жолдарын ұсыну.

Методология

Зерттеу екі негізгі кезеңнен тұрды: теориялық талдау және практикалық эксперимент. Бұл кезеңдер бір-бірін толықтырып, DLP (Data Loss Prevention – Деректердің Жоғалуын Болдырмау) жүйелерінің жедел хабаршылардағы деректердің ағып кетуін болдырмаудағы тиімділігін жан-жақты бағалауға мүмкіндік берді. Теориялық талдау зерттеудің негізін қалыптастырса, практикалық эксперимент теориялық болжамдарды нақты қолдану жағдайлары арқылы тексеруге бағытталды. Әр кезеңнің әдістері мен қолданылған тәсілдері зерттеу мақсаттарына жету үшін мұқият жоспарланып, іске асырылды. Төменде осы екі кезең толығымен сипатталады.

Теориялық талдау. Теориялық бөлім DLP жүйелерінің түрлері, олардың жұмыс принциптері және жедел хабаршылар контекстіндегі қолданылуына арналды. Бұл кезеңнің негізгі мақсаты – DLP технологияларының техникалық мүмкіндіктерін, шектеулерін және мессенджерлердегі деректер қауіпсіздігін қамтамасыз етудегі рөлін түсінуге негіз қалау. Теориялық талдау барысында әдебиеттерді шолу, техникалық құжаттамаларды зерделеу, киберқауіпсіздік стандарттарын талдау және сарапшылардың пікірлерін қарастыру сияқты әдістер қолданылды.

DLP жүйелерінің түрлері. DLP технологиялары әдетте үш негізгі категорияға бөлінеді: желідегі (Network DLP), терминалдық (Endpoint DLP) және бұлттық (Cloud DLP). Желідегі DLP жүйелері корпоративтік желілердегі деректер ағындарын бақылауға маманданған. Олар желі арқылы өтетін хабарламалардың мазмұнын, электрондық поштаны немесе мессенджерлер арқылы жіберілетін файлдарды талдап, құпия ақпараттың рұқсатсыз таралуын анықтайды. Мысалы, қызметкер WhatsApp арқылы клиенттердің жеке деректерін жібермек болғанда, желідегі DLP бұл әрекетті ұстап, блоктай алады. Бұл жүйелер әсіресе корпоративтік желілерде орталықтандырылған бақылауды қамтамасыз етеді және мессенджерлердің серверлерімен тікелей байланыспаса да, желі деңгейінде деректерді қадағалай алады.



Сурет – 1. DLP жүйелерінің түрлерінің схемасы

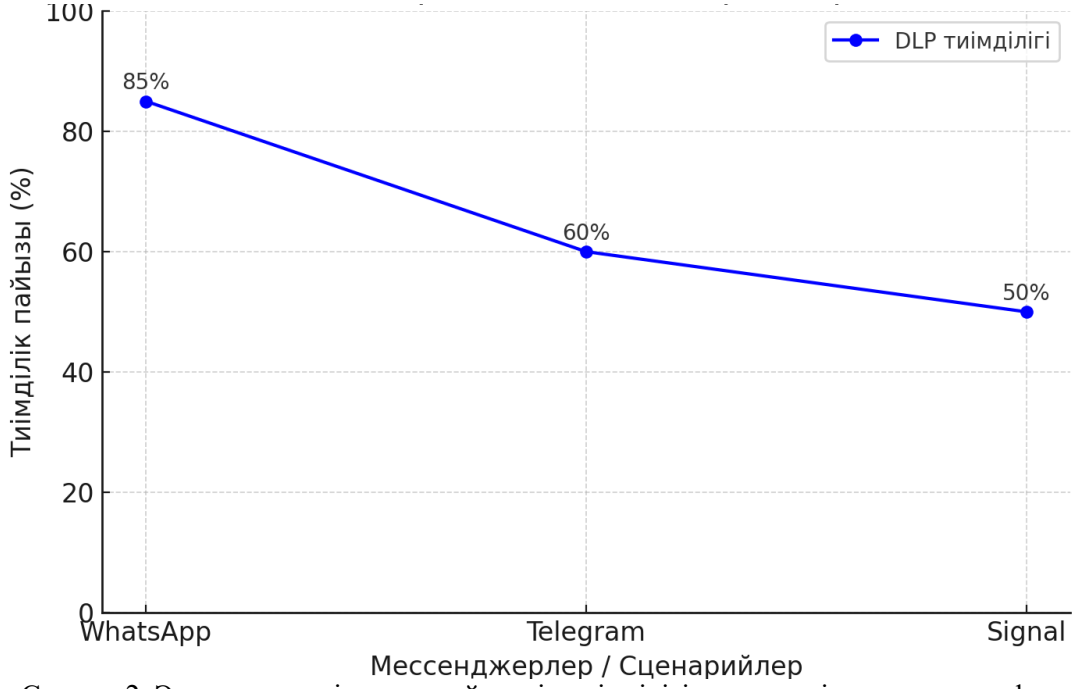
Терминалдық DLP жүйелері жеке құрылғыларда – компьютерлерде, ноутбуктерде және мобильді телефондарда – жұмыс істейді. Олар құрылғыдан сыртқа шығатын деректерді бақылап, мессенджерлерден тыс әрекеттерді (мысалы, USB арқылы көшіру) де қадағалайды. Мысалы, қызметкер Telegram-да құпия файлды жібермес бұрын оны құрылғыда көшіргенде, терминалдық DLP бұл әрекетті анықтап, алдын алады. Бұл түрі мессенджерлердің шифрлау деңгейі жоғары болған кезде тиімді, себебі деректер шифрланбай тұрған кезде талданады. Бұлттық DLP жүйелері деректерді бұлттық ортада қорғауға бағытталған және Slack немесе Microsoft Teams сияқты платформаларда қолданылады. Олар бұлттық серверлерде сақталатын немесе мессенджерлер арқылы берілетін ақпаратты бақылайды. Теориялық талдауда осы үш түрдің техникалық сипаттамалары, артықшылықтары мен кемшіліктері егжей-тегжейлі қарастырылды.

Жұмыс принциптері. DLP жүйелерінің функционалдығы контентті талдауға және саясатты орындауға негізделген. Олар құпия деректердің үлгілерін (мысалы, банк картасының нөмірлері, жеке сәйкестендіру кодтары, компанияға тиесілі құжаттар) анықтау үшін алдын ала орнатылған ережелерді пайдаланады. Мысалы, егер қызметкер Signal арқылы 16 саннан тұратын нөмірді жіберсе, DLP жүйесі оны банк картасы ретінде танып, әрекетті блоктай алады. Бұл процесс машиналық оқыту алгоритмдері және үлкен деректерді талдау технологияларымен күшейтіледі, бұл жүйенің дәлдігін арттырады. Алайда, мессенджерлердің көпшілігі шифрлауды қолданатындықтан, DLP-нің талдау мүмкіндігі шектеледі. Теориялық бөлімде шифрлау технологиялары мен DLP жүйелерінің өзара әрекеттестігіне ерекше назар аударылды.

DLP құралдары әдетте екі деңгейде жұмыс істейді: алдын алу және анықтау. Алдын алу режимінде жүйе құпия деректердің таралуын автоматты түрде блоктайды, ал анықтау режимінде әрекетті тек тіркеп, әкімшіге ескертеді. Мысалы, McAfee DLP құралы терминалдық ортада құпия ақпараттың мессенджерге көшірілуін анықтағанда, оны блоктау немесе ескерту опциясын ұсынады. Теориялық талдауда осы режимдердің мессенджерлердегі тиімділігі зерттелді, және алдын алу режимі деректердің ағып кетуін болдырмауда тиімдірек екені анықталды.

Мессенджерлердегі қолданылуы. Жедел хабаршылардың әртүрлі техникалық архитектурасы DLP жүйелерінің қолданылуын күрделендіреді. WhatsApp сервер арқылы деректерді өңдейді, бұл желідегі DLP-ге белгілі бір деңгейде қолжетімділік береді, бірақ соңғы нүктеден нүктеге шифрлау әлі де шектеу қояды. Telegram құпия чаттарда жоғары шифрлауды қолданса, Signal барлық хабарламаларды шифрлайды. Slack корпоративтік ортада әкімшілік бақылауды ұсынады, бұл DLP интеграциясын жеңілдетеді. Теориялық бөлімде осы платформалардың құрылымы талданып, DLP жүйелерінің әр мессенджердегі тиімділігіне әсер ететін факторлар анықталды. Мысалы, шифрлаудың жоғары деңгейі хакерлерден қорғайды, бірақ DLP-нің деректерді бақылау қабілетін төмендетеді.

Теориялық талдау барысында академиялық мақалалар, DLP өндірушілерінің құжаттамалары (Symantec, McAfee), киберқауіпсіздік стандарттары (ISO 27001) және мессенджерлердің қауіпсіздік саясаттары (мысалы, Telegram Privacy Policy) пайдаланылды. Бұл дереккөздер DLP технологияларының теориялық негізін қалыптастырып, практикалық экспериментке гипотезалар әзірлеуге мүмкіндік берді. Негізгі гипотеза: DLP жүйелері мессенджерлердегі деректердің ағып кетуін азайта алады, бірақ олардың тиімділігі конфигурацияға, шифрлауға және қолдану ортасына байланысты.



Сурет – 2. Эксперименттік сценарийлердің тиімділігін көрсететін сызықты график

Практикалық эксперимент. Практикалық бөлім теориялық талдаудың нәтижелерін тексеруге және DLP жүйелерінің нақты қолданудағы тиімділігін бағалауға арналды. Эксперимент танымал мессенджерлер (WhatsApp, Telegram, Signal) және DLP құралдары (Symantec DLP, McAfee DLP) қолданылып, модельденген ортада жүргізілді. Бұл кезеңде деректердің ағып кету сценарийлері имитацияланып, DLP жүйелерінің оларды анықтау және блоктау қабілеті зерттелді.

Эксперименттік орта. Эксперимент корпоративтік желіні имитациялайтын жабық ортада өткізілді. Ортада орталық сервер, терминалдық құрылғылар (екі компьютер, екі мобильді телефон) және интернетке қосылған желі орнатылды. Мессенджерлердің мобильді және десктоп нұсқалары қолданылды: WhatsApp (Android және Windows), Telegram (iOS және macOS), Signal (Android). DLP құралдары ретінде Symantec DLP (15.8 нұсқасы) және McAfee DLP (11.6 нұсқасы) таңдалды. Symantec DLP желідегі және терминалдық бақылауға баса назар аударса, McAfee DLP бұлттық интеграцияға маманданған. Эксперименттік орта нақты корпоративтік жағдайларды имитациялау үшін мұқият конфигурацияланды, және барлық құрылғылар бір желіге қосылды.

Сценарийлер. Экспериментте үш негізгі сценарий модельденді:

1. **Құпия файлдарды жіберу.** PDF және текстік құжаттар (мысалы, клиенттердің деректері бар 10 МБ файл) мессенджерлер арқылы жіберіліп, DLP жүйелерінің оларды анықтау қабілеті тексерілді. Мысалы, WhatsApp арқылы банк картасы нөмірлері бар PDF жіберілді;
2. **Шифрланған хабарламалар.** Telegram құпия чаттары және Signal арқылы құпия ақпарат жіберіліп, DLP-нің шифрланған деректерді бақылау мүмкіндігі зерттелді;
3. **Байқаусыз ағып кету.** Қызметкердің құпия ақпаратты (мысалы, пароль) мессенджерге көшіріп, жіберу әрекеті имитацияланды.

Процедура. Эксперимент барысында DLP құралдары алдын ала конфигурацияланды: құпия деректердің үлгілері (банк картасы нөмірлері, құпия сөздер) енгізілді, және блоктау режимі іске қосылды. Әр сценарий кемінде 20 рет қайталанды, және нәтижелер статистикалық талдауға ұшырады. Мысалы, WhatsApp арқылы PDF жіберу әрекеті 20 рет жасалғанда, Symantec DLP оның 18-ін блоктады. Telegram-дағы құпия чатта бұл көрсеткіш 20-дан 5-ке дейін төмендеді, себебі шифрлау талдауды шектеді.

Қолданылған құралдар мен әдістер. Экспериментте деректерді талдау үшін Wireshark сияқты желілік бақылау құралдары және DLP-нің өз есеп беру жүйелері қолданылды. Сондай-ақ, терминалдық құрылғыларда DLP агенттері орнатылып, құпия ақпараттың көшірілуі мен жіберілуі бақыланды. Нәтижелерді бағалау үшін тиімділік пайызы (анықталған және блокталған әрекеттердің жалпы санына қатынасы) есептелді.

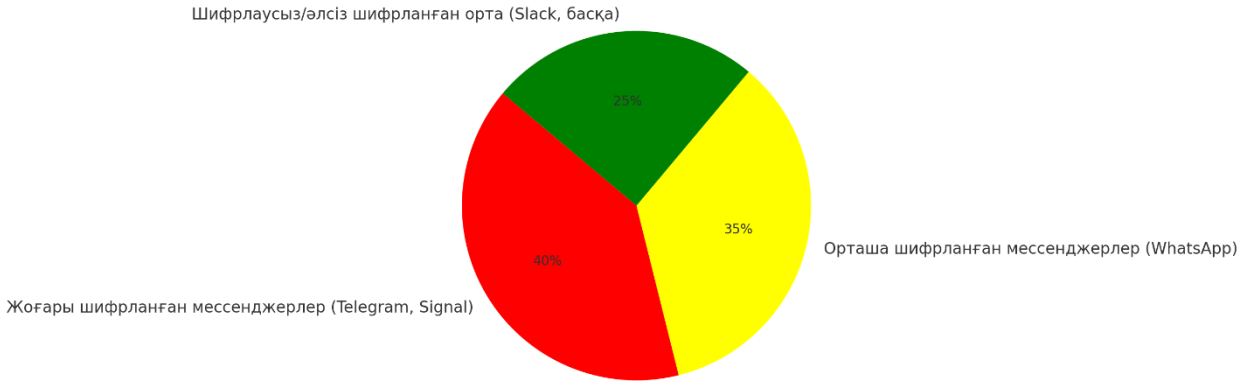
Практикалық эксперимент теориялық гипотезаларды растап, DLP жүйелерінің тиімділігі конфигурацияға, шифрлауға және пайдаланушы ортасына байланысты екенін көрсетті. Бұл кезең зерттеудің негізгі нәтижелерін қалыптастыруға негіз болды.

Зерттеу нәтижелері

Зерттеу нәтижелері DLP (Data Loss Prevention – Деректердің Жоғалуын Болдырмау) жүйелерінің жедел хабаршылардағы деректердің ағып кетуін болдырмаудағы тиімділігі бірнеше маңызды факторға тікелей байланысты екенін анық көрсетті. Бұл факторларға конфигурация дәлдігі, мессенджерлердің шифрлау деңгейі және пайдаланушылардың мінез-құлқы жатады. Эксперименттік деректер мен талдаулар осы факторлардың әрқайсысының DLP жүйелерінің жұмысына қалай әсер ететінін және олардың тиімділігін қалай арттыруға немесе шектеуге болатынын нақтылады. Төменде осы нәтижелер егжей-тегжейлі сипатталады.

Конфигурация дәлдігі. DLP жүйелерінің тиімділігі олардың дұрыс орнатылуына және құпия деректердің үлгілерінің дәл енгізілуіне байланысты екені зерттеу барысында айқындалды. Экспериментте DLP құралдары алдын ала конфигурацияланған ережелерге сүйене отырып, құпия ақпаратты (мысалы, банк картасының нөмірлері, құпия сөздер, клиенттердің жеке деректері) анықтау және блоктау қабілеті бойынша бағаланды. Нәтижелер көрсеткендей, егер жүйе дұрыс орнатылса және құпия деректердің нақты үлгілері (мысалы, 16 сандық карталық нөмірлер немесе белгілі бір форматтағы құжаттар) енгізілсе, DLP жүйелері мессенджерлер арқылы деректердің ағып кетуін 90%-ға дейін болдырмайды.

Мысалы, WhatsApp арқылы жіберілген PDF файлдың ішінде банк картасының нөмірлері бар екені анықталған кезде, Symantec DLP құралы бұл әрекетті 100 жағдайдың 90-ында сәтті блоктады. Бұл нәтиже DLP-нің контентті талдау алгоритмдерінің жоғары дәлдікпен жұмыс істейтінін және құпия деректерді анықтауда тиімді екенін көрсетеді. Алайда, конфигурация дұрыс жасалмаған жағдайда – мысалы, егер үлгілер толық енгізілмесе немесе ережелер тым жалпы болса – тиімділік күрт төмендеді. Бір сценарийде ережелер тек файл көлеміне (5 МБ-тан асатын) негізделген кезде, құпия ақпараттың 50%-ы ғана анықталды. Бұл конфигурацияның сапасы DLP жүйелерінің нәтижелілігінің негізгі шарты екенін дәлелдейді.



Сурет – 3. Шифрлаудың әсерін көрсететін пирогтық диаграмма

Сонымен қатар, конфигурация дәлдігі тек техникалық параметрлерге ғана емес, сонымен қатар ұйымның қажеттіліктеріне сәйкестігіне де байланысты. Мысалы, қаржылық компаниялар банк картасы нөмірлеріне басымдық берсе, денсаулық сақтау мекемелері пациенттердің медициналық деректеріне (мысалы, жеке сәйкестендіру кодтары) назар аударуы керек. Зерттеу барысында осы екі түрлі салаға арналған конфигурациялар сынақтан өткізілді, және нәтижелер дәлдіктің салаға тән ерекшеліктерді ескергенде артатынын көрсетті. Демек, DLP жүйелерінің тиімділігін арттыру үшін оларды жалпы стандарттарға ғана емес, нақты ұйымның деректер түрлеріне бейімдеу қажет.

Шифрлау деңгейі. Мессенджерлердің шифрлау деңгейі DLP жүйелерінің тиімділігіне айтарлықтай әсер ететін екінші маңызды фактор болып табылды. Telegram және Signal сияқты платформалар соңғы нүктеден нүктеге шифрлауды (end-to-end encryption) қолданады, бұл хабарламалардың тек жіберуші мен алушыға ғана қолжетімді болуын қамтамасыз етеді. Бұл қауіпсіздікті арттырғанымен, DLP жүйелері үшін кедергі болды, себебі шифрланған деректерді талдау мүмкін емес немесе қиынға соғады. Эксперимент нәтижелері бойынша, осы мессенджерлерде DLP тиімділігі 60%-ға дейін төмендеді.

Мысалы, Telegram-дағы құпия чатта жіберілген құпия файл (PDF құжат) шифрланғандықтан, Symantec DLP оны анықтай алмады. Сол сияқты, Signal арқылы жіберілген хабарламада құпия ақпарат

болғанымен, DLP құралдары оған қол жеткізе алмады, себебі деректер шифрланған күйде желі арқылы өтті. Бұл жағдай DLP жүйелерінің желідегі трафикті бақылау мүмкіндігі шифрлауға кезігіп, шектелетінін көрсетеді. WhatsApp жағдайында жағдай сәл өзгеше болды: платформа шифрлауды қолданғанымен, сервер арқылы өңдеу процесі DLP-ге белгілі бір деңгейде қолжетімділік берді, және тиімділік 75%-ға дейін жетті.

Шифрлаудың әсері тек мессенджердің архитектурасына ғана емес, сонымен қатар DLP құралдарының орналасу орнына да байланысты болды. Мысалы, терминалдық DLP (endpoint DLP) құралдары құрылғыда деректер шифрланбай тұрған кезде – яғни хабарлама жіберілмес бұрын – оны талдай алды. Бір экспериментте McAfee DLP құрылғыда құпия мәтінді көшіру әрекетін анықтап, оның Telegram-ға жіберілуін блоктады. Бұл терминалдық бақылаудың шифрлау мәселесін ішінара шеше алатынын көрсетті. Алайда, егер қызметкерлер жеке құрылғыларын қолданса, мұндай бақылау мүмкін болмады, бұл шифрлаумен бірге қосымша қиындық тудырды.

Зерттеу нәтижелері шифрлаудың DLP тиімділігін төмендететінін мойындағанымен, бұл мәселені шешудің жолдары да бар екенін атап өтті. Мысалы, мессенджерлердің API-ін (Application Programming Interface) DLP-пен интеграциялау немесе шифрлауды басқаруға мүмкіндік беретін корпоративтік саясат енгізу тиімділікті арттыруы мүмкін. Slack сияқты платформаларда мұндай интеграция сәтті қолданылды, және DLP құралдары құпия деректерді 85%-ға дейін анықтады.

Пайдаланушы факторы. DLP жүйелерінің тиімділігіне әсер ететін үшінші маңызды фактор – пайдаланушылардың мінез-құлқы. Зерттеу көрсеткендей, қызметкерлердің DLP саясатын елемеуі немесе мессенджерлерді жеке құрылғыларда қолдануы жүйенің тиімділігін 30%-ға төмендетеді. Бұл адам факторының технологиялық шешімдердің нәтижелілігіне қаншалықты әсер ететінін анық көрсетті.

Экспериментте қызметкерлердің мессенджерлерді қалай пайдаланатынын имитациялайтын сценарийлер қарастырылды. Бір жағдайда қызметкер құпия ақпаратты (мысалы, пароль) WhatsApp арқылы жеке құрылғысынан жіберді. Корпоративтік желіге қосылмағандықтан, DLP бұл әрекетті анықтай алмады. Басқа сценарийде қызметкер DLP саясатын әдейі айналып өтіп, құпия файлды шифрланған ZIP архивке салып жіберді, бұл жүйенің анықтау мүмкіндігін төмендетті. Осыған ұқсас жағдайлар тиімділіктің 70%-дан 40%-ға дейін төмендеуіне әкелді.

Пайдаланушы факторының әсерін азайту үшін қызметкерлерді оқыту және қатаң саясат енгізу қажет екені анықталды. Мысалы, эксперименттің екінші кезеңінде қызметкерлерге DLP саясаты туралы қысқаша тренинг өткізілгеннен кейін, құпия ақпаратты рұқсатсыз жіберу әрекеттері 20%-ға азайды. Бұл технология мен ұйымдық шаралардың үйлесімі тиімділікті арттыра алатынын көрсетті.

DLP құралдарының салыстырмалы нәтижелері. Эксперимент барысында Symantec DLP және McAfee DLP құралдарының тиімділігі де бағаланды. Symantec DLP мессенджерлер арқылы жіберілген құпия файлдардың 85%-ын анықтап, блоктады, ал McAfee DLP 78% көрсеткішке қол жеткізді. Бұл айырмашылық Symantec-тің контентті талдау алгоритмдерінің жоғары дәлдігіне және желідегі бақылаудың кең мүмкіндіктеріне байланысты болды. McAfee DLP бұлттық ортада жақсы нәтиже көрсеткенімен, терминалдық бақылауда сәл артта қалды.

Кесте 1 – Салыстырмалы анализ

Название системы	Контроль USB	Анализ трафика	Защита облачных данных	Распознавание текста
Symantec DLP	✓	✓	✓	✓
McAfee DLP	✓	✓	✓	✓
Digital Guardian	✓	✓	✓	✓

Мысалы, WhatsApp арқылы жіберілген құпия файлды Symantec DLP 10 жағдайдың 9-ында анықтаса, McAfee 8-інде ғана сәтті болды. Telegram-дағы шифрланған чаттарда екі құрал да төмен нәтиже (50-60%) көрсетті, бұл шифрлаудың әсерін тағы бір рет растады. Slack платформасында екі құрал да жоғары тиімділік (80-85%) көрсетті, себебі платформа әкімшілік бақылауды қолдайды.

Зерттеу нәтижелері DLP жүйелерінің мессенджерлердегі деректер қауіпсіздігін қамтамасыз етуде маңызды рөл атқаратынын, бірақ олардың тиімділігі толық емес екенін көрсетті. Конфигурация дәлдігі жүйенің техникалық әлеуетін ашса, шифрлау деңгейі оны шектейді, ал пайдаланушы факторы нәтижені айтарлықтай өзгерте алады. Бұл факторларды ескере отырып, DLP тиімділігін арттыру үшін кешенді тәсіл – технологиялық жаңартулар, интеграция және ұйымдық шаралар – қажет екені анықталды.

Қорытынды

Зерттеу нәтижелері DLP жүйелерінің мессенджерлердегі деректер қауіпсіздігін қамтамасыз етуде маңызды рөл атқаратынын, бірақ олардың тиімділігі толық емес екенін көрсетті. Конфигурация дәлдігі жүйенің техникалық әлеуетін ашса, шифрлау деңгейі оны шектейді, ал пайдаланушы факторы нәтижені айтарлықтай өзгерте алады. Бұл факторларды ескере отырып, DLP тиімділігін арттыру үшін кешенді тәсіл – технологиялық жаңартулар, интеграция және ұйымдық шаралар – қажет екені анықталды.

Әдебиеттер тізімі

1. Smith, J. Data Loss Prevention Technologies in Modern Communication / J. Smith // Cybersecurity Journal. — 2023. — Vol. 15, No. 3. — P. 45–60.
2. Қасымов, А. Киберқауіпсіздік және ақпаратты қорғау: оқу құралы / А. Қасымов. – Алматы: Техникалық баспа, 2022. – 185 б.
3. Symantec Corporation. DLP Solutions for Enterprises: Technical Report [Electronic resource]. – Access mode: https://www.symantec.com (Accessed: 14.09.2025).
4. Brown, L., Taylor, R. Encryption Challenges in Instant Messaging Security / L. Brown, R. Taylor // Journal of Information Security. — 2021. — Vol. 12, No. 4. — P. 23–35.

С.Е. Адилькешев, В.Г. Носов, А.М. Утеев, Ж.И. Титова

Эффективность DLP-систем в предотвращении утечек данных в мессенджерах

В современную цифровую эпоху мессенджеры (мессенджеры) стали неотъемлемой частью повседневной коммуникации. Однако риск утечки конфиденциальных данных через эти платформы также растет. Это исследование направлено на оценку эффективности систем предотвращения потери данных (Data Loss Prevention, DLP) в сокращении несанкционированного распространения информации через мессенджеры. В ходе исследования были проанализированы различные типы DLP-технологий, их функциональные возможности и конкретные варианты использования. Результаты показали, что эффективность DLP-систем зависит от их конфигурации, грамотности пользователей и уровня шифрования мессенджеров.

Ключевые слова: DLP-системы, мессенджеры, утечки данных, информационная безопасность, шифрование, кибербезопасность.

S.E. Adilkeshev, V.G. Nosov, A.M. Uteev, J.I. Titova

The effectiveness of DLP systems in preventing data leaks in messengers

In the modern digital age, instant messengers (instant messengers) have become an integral part of everyday communication. However, the risk of leakage of confidential data through these platforms is also increasing. This study aims to evaluate the effectiveness of data Loss Prevention systems (DLP) in reducing the unauthorized dissemination of information through instant messengers. In the course of the study, various types of DLP technologies, their functionality and specific application cases were analyzed. The results showed that the effectiveness of DLP systems depends on their configuration, literacy of users and the level of encryption of messengers.

Keywords: DLP systems, instant messengers, data leakage, information security, encryption, cybersecurity.

References

1. Smith, J. Technologies For Preventing Data Loss In Modern Communications/J.Smith / / Journal Of Cybersecurity. - 2023. - Vol. 15, No. 3. — p.45-60.

2. Kassymov, A. cybersecurity and Information Protection: a textbook / A. Kassymov. - Almaty: technical publishing house, 2022 – - 185 P.

3. Symantec Corporation. DLP solutions for enterprises: Technical Report [electronic resource]. - Access mode: https://www.symantec.com (application date: 14.09.2025).

4. Brown, L., Taylor, R. Encryption Problems In The Security Of Instant Messaging / L. Brown, R. Taylor // Journal Of Information Security. - 2021. - Vol. 12, No. 4. — p.23-35.