ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2023»
XVIII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XVIII Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2023»

PROCEEDINGS
of the XVIII International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2023»

2023
Астана

УДК 001+37
ББК 72+74
G99

«ǴYLYM JÁNE BILIM – 2023» студенттер мен жас ғалымдардың XVIII Халықаралық ғылыми конференциясы = XVIII Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2023» = The XVIII International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2023». – Астана: – 6865 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-337-871-8

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001+37
ББК 72+74

ISBN 978-601-337-871-8

ӘОЖ 004.056

"БҰЛТТЫ" ӨНІМДЕРМЕН ЖҰМЫС ІСТЕУ КЕЗІНДЕГІ ҰЙЫМДАРДЫҢ АҚПАРАТТЫҚ ЖҮЙЕЛЕРІНІҢ ҚАУІПСІЗДІГІН БАҒАЛАУ

Абаева Аружан Русланқызы
aru.ruslanqyzy@mail.ru
Л.Н.Гумилев атындағы ЕҰУ, Ақпараттық технологиялар факультеті,
6В06306 – Ақпараттық қауіпсіздік жүйелері мамандығының 3 – курс студенті
Ғылыми жетекшісі – Қанжекеев А.С.

Ақпарат – кез-келген ұйым үшін ең негізгі ресурс. Қызметтердің дұрыс орындалуы ақпараттың сақталуы мен қол жетімділігіне тікелей байланысты. Ақпарат оған иелік ететін адамдарға байланысты оң немесе теріс әсер етеді. Сондықтан көбінесе ақпарат бәсекелестердің, бұзақылардың, қарақшылардың шабуылына жиі ұшырайды.

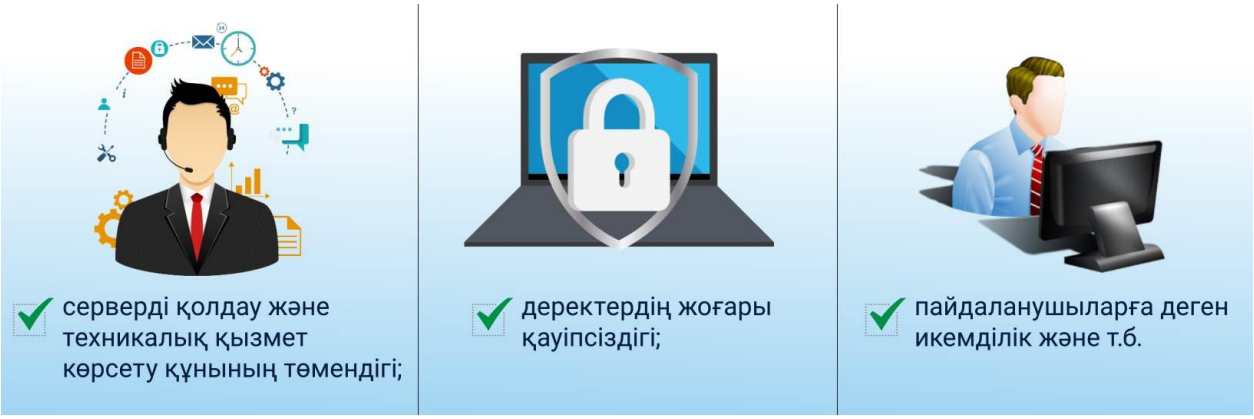
Бастапқы кезде ұйымдардың ақпараттық жүйелері нақты құжаттар түрінде үлкен мұрағаттарда сақталған болатын. Мұндай ақпараттық жүйелердің қауіпсіздігі ақпарат сақталатын орынға кірудің шектелуі арқылы қамтамасыз етілген.

Ақпараттық технологияның пайда болуы көп нәрсені өзгертті. Ақпаратқа қол жеткізуді шектеудің жаңа тәсілдері пайда болды, оны өңдеу және бөлісу тәсілдері оңайырақ әрі жылдамырақ болды. Дегенмен, қауіпсіздік мәселесі өзекті болып қала береді. Ақпарат барлық ықтимал қауіптерге әлі де осал.

Кез-келген ұйымда өз қызметін жүргізу үшін ақпаратқа үлкен көңіл бөлінеді. Ұйымдардың жұмысына түрлі автоматтандырылған ақпараттық жүйелер енгізіліп жатыр. Алайда олардың ақпаратқа қол жеткізу бағдарламалық код деңгейінде шектелген. Антивирустық бағдарламалар мен бағдарламалар кешені барлық жерде қолданылады, олар әр жұмыс орнын және жалпы жергілікті желіні түрлі вирустардан қорғайды. Қорғалған желілік қосылымдар, желіаралық экрандар қолданылады.

Алайда, қазіргі заманғы технологиялар неғұрлым дамыған сайын ақпаратты жан-жақты қорғау қажеттілігі де туындады.

Соңғы бірнеше жылда бұлтты есептеу және виртуализация тұжырымдамасы күшейіп, ақпараттық технологиялар саласында танымал болды. Бұл тұжырымдамаға деген қызығушылық оның өзіне тән артықшылықтарына байланысты, мысалы: (Сурет 1.)



Сурет 1. Бұлтты қызметтердің тиімділігі

Бұлтты қызметтер жұмыс үшін, ғылымда, денсаулық сақтауда, жеке өмірде қолданылады. Әрбір адам және кез келген компания жасайтын деректердің үлкен көлемін сақтау қажет. Бұлтты технологияларды қолдану бизнеске бағдарламалық жасақтаманы, аппараттық құралдарды және

электр энергиясын үнемдеуге мүмкіндік береді деп саналады. Қаражат көп үнемделеді, өйткені бұл кез-келген ұйымның өте қымбат бөлігі, бизнесті одан әрі дамытуға жұмсалуы мүмкін.

Осы технологияны пайдалану қауіпсіздігіне қатысты бірқатар мәселелер бар, көптеген компания әлі күнге дейін оған сенбейді, кез-келген уақытта қолда бар ақпаратпен кез-келген әрекетті жасай отырып, бәрін өзімен бірге ұстауды жөн көреді.

Сондықтан, ұйымдарда "бұлтты" технологияларды пайдалану қауіпсіздігіне қатысты барлық мәселелерді мүмкіндігінше терең түсіну және ақпараттық қауіпсіздік тұрғысынан осы технологияны қолдануға қатысты кейбір ұсыныстарды әзірлеу қажет.

1. "Бұлтты" технологиялардың негізгі сипаттамаларын, қызмет көрсету үлгілері мен түрлерін және олардың ұйымдардың қызметіне әсерін талдасақ,

"Бұлтты" технологияның негізгі сипаттамалары:

- талап бойынша өзіне-өзі қызмет көрсету;
- желі арқылы әмбебап қол жетімділік;
- ресурстарды біріктіру;
- икемділік;
- ресурстар мен қуаттарды тұтынуды есепке алу.

Кесте. 1 "Бұлтты" технологияның сипаттамалары

+ Оң әсері:	**- Теріс әсері:**
қол жетімділік;	желіге тұрақты қосылу;
құнының төмендігі;	"бұлтта" қолданылатын бағдарламалық жасақтамаға шектеулер;
икемділік (пайдаланылған ресурстардың шексіздігі);	құпиялылық;
сенімділік (резервтік қуат көздері, резервтік көшірмелер, шабуылға төзімділік);	сенімділік (қалпына келтіру мүмкіндігі жоқ ақпараттың жоғалуы);
қауіпсіздік (тиісті қамтамасыз ету кезінде).	қауіпсіздік (вирустардың ену мүмкіндігі).

2. "Ақпараттық қауіпсіздік" ұғымы, ақпараттық қауіпсіздік қатерлері, ұйымдағы ақпараттық қауіпсіздікті қамтамасыз етуге қойылатын талаптар.

Ақпараттық қауіпсіздіктің 3 негізгі міндеттері:

- тұтастықты қамтамасыз ету;
- қолжетімділікті қамтамасыз ету;
- құпиялылықты қамтамасыз ету.

Бұлттағы ақпаратты қорғау стратегиясы – бұл деректердің енуі мен бұзылуын болдырмау әдістерінің жиынтығы. Деректерді қорғау стратегиясы бұлтты компанияны немесе қарапайым пайдаланушыны кімнің пайдаланатынына да байланысты болады.

Ұйымдағы ақпараттық қауіпсіздікті қамтамасыз етуге қойылатын талаптар:

- ақпараттық жүйенің қауіпсіздігі тәуекелдері мен қауіптеріне тұрақты бағалау жүргізу;
- АЖ-да қолданылатын қауіпсіздік реттегіштерінің тұрақты мониторингі;
- қауіпсіздікті бұзушыларға санкциялар қолдану;
- қызметкерлерді оқыту;
- АЖ-ға қол жеткізуді басқару;
- АЖ жұмыс істеуі үшін қажетті жағдайларды қамтамасыз ету;
- АЖ-ны зиянды бағдарламалардан қорғау және т.б.

3) "Бұлтты" өнімдермен жұмыс істеу кезінде ұйымның қауіпсіздігін бағалау.

Бұлттардағы қауіпсіздік мәселелерінің негізгі себептерінің ішінде келесілерді атап өтуге болады:

- бұлтты инфрақұрылымға көшу кезінде қауіпсіздік периметрі ұғымы бұлыңғыр болады;

- фокусты қауіпсіздіктен сенімділікке ауыстыру;
- ресурстарды әртүрлі тұтынушылармен бөлісу;
- бұлтты есептеу қызметтерін пайдалану кезінде тұтынушы провайдерге айтарлықтай тәуелді болады.

Ұйым жұмысында "бұлтты" технологияларды қолданудың келесі негізгі тәуекелдері бар:

- деректерді бақылауды жоғалту;
- деректерді қалпына келтіру;
- зиянды инсайдерлер;
- ескі технологияларды қолдану;
- деректердің ағуы және жоғалуы;
- бұлт инфрақұрылымының қауіпсіздігі;
- байланыс сапасы.

Қауіпсіздікті басқарудың тиімді әдістері:

- DDoS басқару элементтері, сыртқы немесе CSP Azure DDoS немесе AWS DDoS және AWS Shield;
- CDN (мазмұнды тарату желісі) немесе Azure CDN немесе AWS CloudFront сияқты ұқсас трафикті тарату жүйелері;
- DNS қорғанысы, мысалы, Azure трафик менеджері немесе AWS 53 бағыты;
- Azure WAF немесе AWS WAF сияқты веб-қосымшалардың брандмауэрлері;
- Azure NSG немесе AWS Security Groups қол жеткізуді, рөлдерді және рұқсаттарды басқару.

Үшінші тарапқа құпия ақпаратты сеніп тапсырудан бұрын, бұлтты қызмет провайдерінің қауіпсіздігін қамтамасыз ету деңгейіне қатысты барлық қол жетімді материалдармен танысу қажет.

"Бұлттардың" минималды қауіпсіздігін қамтамасыз етуге қойылатын талаптар:

- физикалық қорғау-дата-орталықтарды қорғау (объектідегі күзет, өткізу режимі, жабдықты пайдаланудың талап етілетін жағдайларын қолдау, тәулік бойы қызмет көрсету);
- ресурстарды физикалық бөлу - күшейтілген қорғауды қажет етпейтін жалпы инфрақұрылымнан бөлек маңызды деректерді өңдеу;
- антивирустық қорғаныс;
- жүйенің қауіпсіздігі - виртуалды машиналар мен ОЖ үшін брандмауэрлердің болуы;
- осалдықтан қорғау - жалпы осалдықтарға шабуыл жасауға дайын болу;
- деректер қауіпсіздігі - деректерге қол жеткізуді басқару;
- аутентификация – пароль\логинін пайдалану, аутентификация процесін шифрлау. Пайдаланушыларды рөлдер бойынша бөлу қажет, яғни авторизация;
- өзгерістерді бақылау – екі тарап та жүйедегі өзгерістерден хабардар болуы керек;
- шифрлау - бұлттағы деректерді шифрлау;
- өңдеу және сақтау заңға сәйкес болуы керек.

Қарапайым пайдаланушылар бұлтты қызметтерді үнемі пайдаланады. Достарға пошта немесе фотосуреттер жібергенде, біз «бұлт» технологиясының көмегіне жүгінеміз. Бұл жағдайда пайдаланушы әрқашан оның архитектурасының элементтерінің бірін - веб-интерфейсті пайдаланады.

Веб-интерфейсті күшейту керек, себебі бұл шабуыл жасалуы мүмкін қосымшаның бірінші компоненті. Аутентификация беті қарапайым болуы керек және сыртқы сәйкестендіру жазбасын, сондай-ақ авторизация белгілерін қамтуы мүмкін.

Зерттеу нәтижелері бойынша, «бұлтты өнімдерді пайдалану қауіпсіздігі туралы консенсус жоқ» деген қорытынды жасауға болады. Қазіргі уақытта адамдар екі «топқа» бөлінеді – қолдайтындар және мүлдем қарсы. Провайдерлерге деген сенімсіздік те бар. Көбі бұлтты қоймаға түскен құпия ақпаратты (соның ішінде жеке деректерді) олар өз қалауы бойынша басқаратынына ("бақылау") сенімді.

Бұлттарды ұйымдардың қызметіне енгізу кезінде жалпы ақпараттық қауіпсіздікті қамтамасыз етуді реттейтін жалпыланған стандарттар, нормативтік актілер мен заңдар қолданылады. Алайда, технологияның ерекшелігі мен оны іске асырудың күрделілігін ескере отырып, бұлтты өнімдермен жұмыс істеу кезінде ақпараттық қауіпсіздікті қамтамасыз етудің әдістерін егжей-тегжейлі қарастыруға бағытталған стандарттар қажет.

Қазіргі таңда осындай құжаттар бар және жаңартылып отырады. Олардың көмегімен, тұтынушылар технологияны және онымен қалай жұмыс істеу керектігін көбірек түсінетін болады. Сервисті ұсыну сапасын жақсартуға бағытталған бағдарламалық қамтама провайдерлері мен әзірлеушілеріне қойылатын белгілі бір талаптар мен шектеулер бар. Бұл қызметтің қауіпсіздік деңгейін де, тұтынушылардың сенім деңгейін де едәуір арттырады деп болжауға болады.

Пайдаланылған әдебиеттер тізімі:

1. “Безопасность и защита данных в облачных технологиях”. https://boodet.online/blog/bezopasnost-i-zashhita-dannyh-v-oblachnyh-tehnologiyah-boodet-onine?ysclid=lerz51fj27108923164

2. У.Шнайдер, “Безопасность при использовании облачных сервисов. Журнал сетевых решений LAN ”.

3. Защита информации в облачных сервисах. URL: https://smoff.ru/howitworks/zashchita-informacii-v-oblachnyh-servisah

4. Что такое безопасность облака? URL: https://www.kaspersky.ru/resource-center/definitions/what-is-cloud-security

ӘОЖ 004.056.57

ПРОГРАММАЛЫҚ ҚАМТАМАНЫҢ ҚҰЖАТТАЛМАҒАН МҮМКІНДІКТЕРІН АНЫҚТАУ ӘДІСТЕРІ МЕН ҚҰРАЛДАРЫН ЗЕРТТЕУ

Альсеитов Олжас Айдосович
olzhas010111@gmail.com
Л.Н.Гумилев атындағы Еуразия ұлттық университеті
ақпараттық-технологиялар факультетінің ақпарат қорғау жүйесі мамандығының 1 курс магистранты
Ғылыми жетекшісі - Туребаева Р.Д. , Сауханова Ж.С.

Кіріспе:

Заманауи ақпараттық технологияларды, есептеу техникасын және телекоммуникациялық жүйелердің негізі болып программалық қамтама болып табылады. Ақпараттық технологиялар қарқынды өсуі адам қызметінің әртүрлі салаларында қолдануы және ақпараттық технологияның адам өмірінің сапалық көрсеткіштеріне ықпалының артуы программалық қамтаманың жұмысының көлемін ұлғайту, үлкен ресурстарды тарту қажеттілігі бойынша сапа және біліктілік талаптарын әзірлеу, арттыру салдарына әкеліп соқтырды. Заман талабына сай ақпараттық технологиялар қарқынды өсуден негізгі ақпарат қорғау ережелеріне және оның жолдарын қолдануға әкелді. Егер бірнеше жыл бұрын программалық қамтама тек функционалды түрде дұрыс және қажетті тапсырмаларды істейтін талаптар қойылса, қазіргі уақытта программалық қамтама құнды ақпарат ағып кетуінен, жүйенің шабуылдарға осал болуынан қорғайды. Программалық қамтаманың маңызды осалдыңы құжатталмаған мүмкіндіктері болып табылады. Негізгі бөлімде құжатталмаған мүмкіндіктерді анықтауға арналған негізгі талдау әдістері мен құралдарына шолу жасаймын және статитикалық талдау негізінде өзімнің жасаған жүйедегі осалдықты анықтау процессін жүргіздім.

Негізгі бөлім:

Бағалау объектісінің осалдықтары мен құжатталмаған мүмкіндіктерін анықтау бойынша жүргізілетін талдауларды:

1. Программалық қамтаманы эксперттік талдау әдістері мен құралдарын зерттеу