МРНТИ 81.93.29
ӘОЖ 004.02 **DOI 10.52167/1609-1817-2023-125-2-390-400**

М. Бақыт, Х. Молдамурат✉, Е.Н. Сейткулов, С.К. Атанов, М.И. Бекенов
Л.Н.Гумилев атындағы Еуразия ұлттық университеті,
Астана, Қазақстан
E-mail:Moldamurat@yandex.kz

СПУТНИКТІК МОБИЛЬДІ ТЕЛЕФОН АРНАСЫНДАҒЫ ДЕРЕКТЕРІ ҮШІН КИБЕРҚАУІПСІЗДІК ҚАУІПТЕРІН ТАЛДАУ

Аңдатпа. Бұл мақалада спутниктік мобильді обьектілер мен мобильді телефондардың арналары, оларды іске асыратын аппаратуралардағы деректер үшін киберқауіпсіздік қауіптерін талдау мен бағдарламалық қорғау мәселелері зерттелді. Ақпараттық телекоммуникалық жүйесіндегі технологиялар мен қолданудың тиімді тәсілдері қарастырылды. Төмен орбиталық ұшу аппараттарының деректері үшін киберқауіпсіздік қауіптерін талдау қарастырылады. Бүгінгі таңда спутниктік киберқауіпсіздік маңызды тақырып болып табылады. Жарналар тарих пен қауіпсіздік зерттеулерінен бастап аэроғарыштық инженерия мен астрофизикаға дейінгі пәндер бойынша бөлінді. Бұл мақала осы пәнаралық үлестерді бөліп көрсетуге және ғарыш жүйелерінің қауіпсіздік мәртебесі туралы білімді жүйелеуге тырысады. Жүйе ғарыштық байланыстың жердегі сегменті үшін ақпараттық қауіпсіздік қауіптерін модельдеуден басталады. Ғарыш жүйелеріне қауіп-қатерлерді шабуылдаушыларды, осалдықтар мен мотивтерді байланыстыратын бірыңғай матрицада сипатталады. Бұл модель спутниктік оқиғалардың толық тарихи уақытымен расталады. Түпкілікті нәтиже - ғарыш жүйелерінің қауіпсіздігін зерттеуді жақтайтындар үшін эмпирикалық және дәлелденген негіз келтіріледі. Қауіптерді модельдеуге, оның ішінде төмен орбиталық ұшақтарды қорғауға теориялық талдау жасалады. Сондай-ақ, төмен орбиталық ұшу аппараттарының деректері үшін қауіптерді модельдеу, қауіптерді модельдеу бойынша семинарды ұйымдастыру және бағалау сипатталады.

Түйінді сөздер. Спутниктік мобильді обьектілер, мобильді телефондардың киберқауіпсіздігі, ғарыштық байланыс арналары, ақпараттық қауіпсіздік, шифрлау, ақпараттық телекоммуникалық жүйе, төмен орбиталық ұшу аппараттары.

Кіріспе.

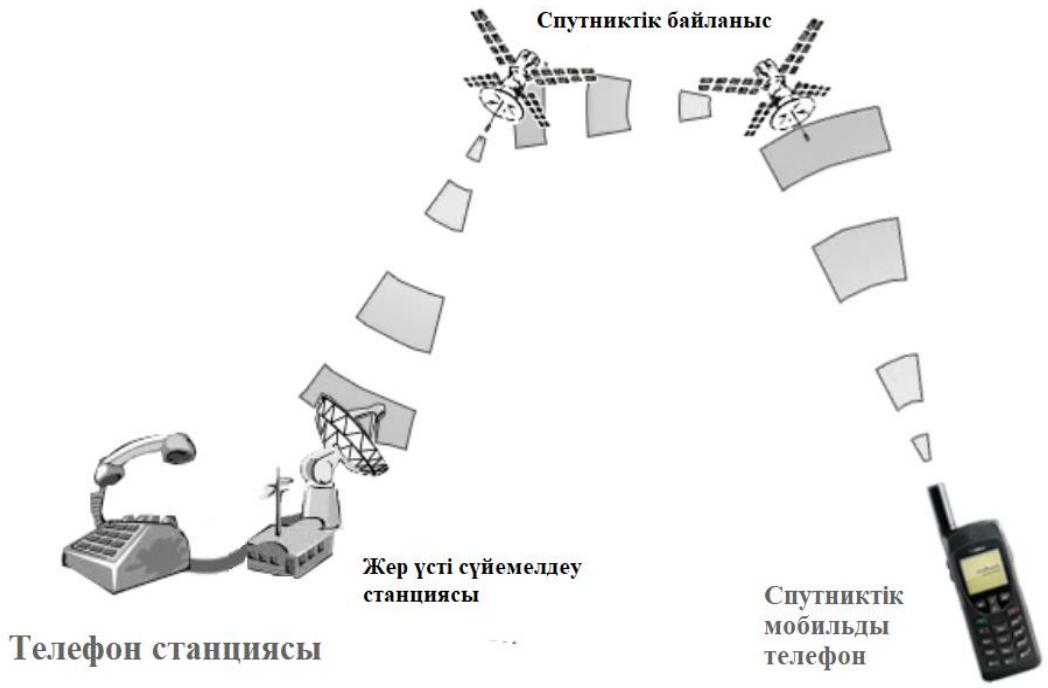
Спутник 1957 жылдың қазан айында ұшырылғаннан бері ғарыштық технологиялар ақпарат ғасырының басталуында шешуші рөл атқарды. Бүгінгі таңда спутниктер тек ғылыми демонстрациялардан әлдеқайда көп, оның орнына олар біздің өмірімізді анықтайтын негізгі қызметтерді қолдайды. Спутниктік индустрия нарығы миниатюризация және ұшыру шығындарын азайту арқылы қайта жанданған сайын, бұл жүйелерді кибершабуылдардан бір уақытта қорғай отырып, кибершабуылдардың құны тек артады.

Бүгінгі таңда спутниктік киберқауіпсіздік маңызды және маңызды емес тақырып болып табылады. Жарналар тарих пен қауіпсіздік зерттеулерінен бастап аэроғарыштық инженерия мен астрофизикаға дейінгі пәндер бойынша бөлінді. Бұл мақала осы пәнаралық үлестерді бөліп көрсетуге және ғарыш жүйелерінің қауіпсіздік мәртебесі туралы білімді жүйелеуге тырысады [1].

Спутниктік байланыс жүйесімен ұялы телефоннан әлемдегі кез келген стационарлық/ұялы 1-ші ұялы телефонға қоңырау шалған кезде сигнал спутниктік 2-ші

ұялы телефоннан спутникке және спутниктен жердегі желілер арқылы деректер орталығы арқылы қоңырау шалу абонентіне өтеді. Сигнал AES 256 стандартына сәйкес шифрланады және аналог-сандық сигналар арқылы құрылығы ортасында спутниктік жүйе арқылы екі абанентке тасмалданады.

Спутниктік байланыс арқылы бірінші ұялы телефоннан екінші спутниктік байланыс арқылы ұялы телефонға қоңырау шалу кезінде мүлдем қоңыраудағы мәлімет тындалмайды.



1 сурет - Спутниктік мобильді байланыс арнасы

Бұл жағдайда сигнал Жерге мүлдем тимейді және спутниктер байланыс арқылы тікелей спутниктік байланыс арнасы арқылы қоңырау ұялы телефонынға өтеді. Жерге, деректер орталығына тек техникалық деректер праметрлері беріледі, мысалы: қоңыраудың ұзақтығы (шоттан қоңырау құнын сақтау үшін) және континентке дейінгі гео-позиция (кейбір тарифтерде әлемнің әртүрлі нүктелеріндегі қоңырау құны әр түрлі болуы мүмкін). Осылайша, спутниктік байланыс арнасы арқылы ұялы телефоннан спутниктік байланыс арнасы арқылы мобильді телефонның қоңырауларын тыңдау мүмкін емес. Сонымен қатар, спутниктік байланыс арнасындағы телефонның сигналы конустық емес, спутниктік байланыс арнасы арқылы іске асатын ұялы телефондардың бағытталған анасы мен ақпараттарды арнайы құралдармен тыңдау немесе сканерлеу мүмкін емес.

Процесс ғарыштық байланыстың жердегі сегменті үшін ақпараттық қауіпсіздік қауіптерін модельдеуден басталады. Ғарыш жүйелеріне қауіп-қатерлерді шабуылдаушыларды, осалдықтар мен мотивтерді байланыстыратын бірыңғай матрицада сипаттаңыз. Бұл модель спутниктік оқиғалардың толық тарихи уақытымен расталады. Түпкілікті нәтиже-ғарыш жүйелерінің қауіпсіздігін зерттеуді жақтайтындар үшін эмпирикалық және дәлелденген негіз.

Біз жер сегментінің табиғи қауіпсіздік таксономиясын ұсыну үшін осы негізге сүйенеміз. Ол үшін біз соңғы техникалық және академиялық әзірлемелер шешілмеген мәселелерді анықтауға көмектесетін қауіп-қатерді модельдеу процесін қолданамыз.

Ғарыштық ұшу қауіпсіздігі мен қауіпсіздігіне байланысты. Бұл әр саладағы перспективалық зерттеу бағыттарын нақты көрсетуді қамтиды [2]. Біз бұл талдауды осы

мақалада техникалық зерттеулерді ынталандыру үшін ғана емес, сонымен қатар осы салада болашақ жұмыс үшін ұшыру алаңы ретінде де қолданамыз.

Материалдар мен тәсілдер.

Эзотерикалық жабдықтар мен шектеулі қол жетімділіктен зардап шегетін ғарыштық платформалардан айырмашылығы, Жердегі жүйелер киберқауіпсіздік туралы көптеген жалпы білімнің пайдасын көреді. Әдетте, спутниктік жерүсті станциялары кез-келген басқа жердегі желілік есептеу жүйелерінен еш айырмашылығы жоқ, ал олар ерекшеленетін жерде жердегі байланыс жүйелеріне ұқсас болып қалады. Іске асырудың әртүрлілігіне қарамастан, барлық Жердегі станциялар кем дегенде радио жабдықтары мен жабдықты басқаратын компьютерден тұрады [3]. Әдетте компьютерде арнайы спутниктік бағдарламалық жасақтамасы бар дәстүрлі операциялық жүйелер жұмыс істейді.

Л. Н. Гумилев атындағы Еуразия ұлттық университеті (бұдан әрі – ЕҰУ) студенттері мен оқытушыларының анық емес логика негізінде қанатты зымырандарды басқарудың интеллектуалды жүйесін әзірлеу және модельдеу, төменгі орбитадағы шағын спутниктер тобын басқарудың бағдарламалық тренажерін әзірлеу, инерциялық навигациялық жүйелерге арналған ұшқышсыз ұшу алгоритмдерін әзірлеу және енгізу, көп агенттік робототехникалық кешендердің қозғалысын үйлестіру, Bluetooth-маяктарға негізделген навигациялық жүйе: іске асыру және эксперименттік бағалау жұмыстары атқарылуда. Сонымен қатар спутниктік байланыс арқылы мобильды телефондардың байланыс арналарын қорғау әдістері жасылынып жатыр және ақпараттық ұорғау әдістері мен оларды алдын алу жұмыстарыда жасалуда.

Сирек жағдайларда бұл мамандандырылған бағдарламалық жасақтама нысанаға айналды. Мысалы, 2000 жылы хакерлер кері инженерлік спутниктерді басқару үшін Exigent бағдарламалық жасақтамасының көшірмелерін ұрлап кетті. Әдетте, шабуылдар мақсатты емес шабуылдардың жанама өнімдері болып табылады (мысалы, 1999 жылы жасөспірім хакер кездейсоқ NASA-ның ұшуды басқару жүйелеріне қол жеткізді). Осыған байланысты Жерүсті станцияларының қауіпсіздігіне өте аз академиялық әдебиеттер арналады [4]. Дегенмен, кейбір ерекше аспектілер назар аударуға тұрарлық.

Біріншіден, спутниктік Жер үсті жүйелері әрқашан дерлік пайдалы жүктемені пайдаланудан қорғаудың соңғы желісі болып табылады. Спутниктік бағдарламалық жасақтама мен аппараттық құралдар әдетте «ашық сенім» моделін ұстанады, онда Жер станциялары ғарыш платформасындағы барлық құрылғыларға сенеді. Осылайша, Жердегі жүйелер миссиялар үшін бір сәтсіздік нүктесін білдіреді. Осы мәселені ескере отырып, Ллансо мен Пирсон компаға келген немесе жоғалған жағдайда басқаруды қалпына келтіру үшін резервтік станцияларды жобалауды ұсынады. Бұл жаңа жер станциясының қызмет ретінде қолданылуының бірі.

Екіншіден, жерсеріктік Жер орталық жүйелері физикалық қорғаныс құралдарына қол жетімділігі шектеулі шалғай аудандарда орналасуы мүмкін. Себебі орналастырудың негізгі пікірі сигналды қамтуға және белгілі бір орбитаға қол жеткізуге байланысты [5]. Көбінесе бұл жерде бірнеше қызметкерлер үнемі қатысады. Оның орнына күнделікті операциялар жоғары дәрежеде автоматтандырылады және орталықтандырылған операциялық орталықтан қашықтан басқарылады.

Бұл физикалық қол жетімділік шабуылдарының қаупін арттырады және көптеген басқа маңызды ақпараттық жүйелерден айырмашылығын алыстырады.

Ақырында, жердегі спутниктік байланыс станциялары әдетте жердегі интернет пен спутниктер арасындағы негізгі «көпір» болып табылады. Қашықтықтан қол жетімділікті көп пайдаланғандықтан, жер үсті станциялары толығымен «ауа саңылауын» қиындатады. Алдыңғы қауіпсіздік зерттеулері жердегі станциялардың бағдарламалық жасақтамасындағы көптеген осалдықтарды анықтады және жердегі терминалдарды

Shodan сияқты IoT іздеу жүйелері арқылы оңай анықтауға болатындығын көрсетті. Сонымен қатар, жер үсті станцияларының салыстырмалы түрде кең таралған жабдықтары кіру кедергілерінің басқа сегменттерге қарағанда төмен екенін білдіреді.

Әдетте, жердегі жүйелерді қорғау үшін корпоративтік қауіпсіздіктің дәстүрлі әдістері тағайындалады. Мысалы, дәстүрлі сот-медициналық құралдарды қолдана отырып, Жердегі станцияда зиянды бағдарламаларға аудит жүргізуге болады [6]. Спутниктік ортаға ғана тән және ұзақ қашықтықтағы радио жабдықтары мен мобильды телефондар сияқты арнайы қауіпсіздік режимін қажет етуі мүмкін кейбір жүйелер бар. Аппараттық жабдыққа және мобильді телефондардың ішкі жүйелері андойдтық жүйелерге жасалған шабуылдардың қоғамдық мысалдарын және осы факторларды шектеулі ғылыми зерттеулерді таппады.

Сондықтан жердегі станциялардың қауіпсіздігі әдетте дәстүрлі ат қауіпсіздігінің кеңеюі болып саналады. Маңызды айырмашылық көбінесе шабуыл мен қорғаныс механизмдерінде емес, ықтимал зиянның ауырлығында болады. Алайда, бұл максимум әмбебап емес. Болашақ қауіпсіздік шабуылдары бұрын жіберіп алған осалдықтарды анықтауға қабілетті бірегей спутниктік басқару аппараттық және бағдарламалық құралына бағытталған. Осы динамиканы зерттеу бағыттарының бірнеше нақты мысалдары 1-кестеде келтірілген.

1 кесте - Жердегі қауіпсіздікті зерттеу бағытының мысалы

Қауіпсіздік мәселесі	Доменге байланысты кедергілер	Тиісті білімнің жекелеген салалары
Деструктивті зиянды бағдарлама немесе жердегі станцияға қарсы «қызмет көрсетуден бас тарту» шабуылы ғарыш миссиясын функционалды түрде оқшаулауы мүмкін.	Жабдықтың жоғары құны операторлардың спутниктерімен бір ғана байланыс нүктесі болуы мүмкін дегенді білдіреді.	Бұлт Қауіпсіздік Таратылған / Жалпы желі сенсоры
Жер станциясының бұзылған компьютері спутникке сенімді ұшуды басқару тобын бере алады.	Орбитада тестілеудің шектеулі мүмкіндіктері тестілеу көбінесе станцияның пайдаланушысына емес, өзіне негізделгенін білдіреді.	РКІ және ЭЦҚ Өнеркәсіптік бақылау Қауіпсіздік жүйесі
Сигналдарды өңдеу жабдықтарындағы артқы есік маңызды деректерді жасырады (мысалы, белгілі бір аймақтың, жиектің фотосуреттері).	Меншікті хаттамалар мен аппараттық компоненттерді қарқынды пайдалану. Жалғыз сәтсіздік нүктесі тек шабуылдаушыларға деректерді беруді емес, оларды қабылдауды манипуляциялау керек дегенді білдіреді.	Жеткізу тізбегі Қауіпсіздік Сигнал Күтім

Нәтижелер.

Ақпараттық теллекоммуникалар және спутниктік қауіп-қатерді модельдеу процедурасы нақты жағдайда тексерілуі керек еді. Huld ғарыштық жобаларға қызмет көрсету шешімі ретінде қауіпсіз Жер сегментін қамтамасыз ету үшін Жер сегментіндегі спутниктік мобильді телефон арналарына негізделген бағдарламалық құралын әзірлеумен айналысқаннан бері ол сынақ орталығы ретінде таңдалды.

Orbitcon үшін сервистік шешім ретінде жер сегменті әзірленуде. Жобаның мақсаты миссияның бүкіл өмірлік циклінде шағын спутниктерді ұшыратын және басқаратын жаңа ғарыштық жобалардың қажеттіліктерін қанағаттандыру үшін ұшуды басқару жүйесін (MCS) құру болды. Қызмет бұлтқа негізделген. Жүйе қолданыстағы жер үсті станцияларын қосу үшін Space Link Extension Protocol (SLE) қолдайды, сонымен қатар оның дизайны VHF, UHF және S-BAND [7] қамтылған.

Бағалау үшін таңдалған әдіс әрекетті зерттеу болды. Іс-әрекетті зерттеу ынтымақтастық пен өзгерістерге бағытталған білімді дамыта отырып, мәселелерді шешуге бағытталған.

Қатерлерді модельдеу бойынша семинар ұйымдастыру

Семинарды ұйымдастыру туралы шешім ұсыныс қабылданып, компания ішіндегі басшылыққа берілгеннен кейін бірден қабылданды. Барлық тараптар жердегі сегментке қауіп-қатерді модельдеу пайдалы және жобаның сәтті болуы үшін қажет деп келісті. Сонымен қатар, қауіп-қатерді модельдеу процедурасы ғарыш саласының басқа сегменттеріне бейімделіп, болашақта тұтынушыларға ұсынылуы мүмкін.

Бірінші қадам мүшелер тізімін жасау болды. Келесі рөлдері бар адамдар шақырылды:

– өнім менеджері;
– әзірлеушілер, үш адам;
– киберқауіпсіздік мамандары, 3 адам;
– ғарыш маманы; сол сияқты
– менеджерлер, үш адам.

Екінші қадам семинардың өтетін күні мен уақытын таңдау болды. Шақыруда кездесудің ауқымы мен мақсаты, сондай-ақ күн тәртібі көрсетілген. Көптеген қатысушылармен қолайлы күнді табу оңай болған жоқ, бірақ кейінге қалдырылғаннан кейін іс-шара бірден барлық шақырылғандарды ұйымдастыратын жаңа күнге ауыстырылды.

Іс-шараны ұйымдастырудағы алғашқы проблема семинар форматы талқылау тақырыбы болған кезде пайда болды. Семинарлар дәстүрлі түрде барлық қатысушылар интерактивті тақтаға кіру мүмкіндігі бар конференц-залда жеке кездескен кезде жақсы жұмыс істейді. Бұл жүйенің схемасын түсінуге және түсінуге көмектеседі, сонымен қатар жаңа идеялардың пайда болуына көмектеседі. Дегенмен, бір бөлмеде физикалық болу жүргізушіге қатысушылардың дене тілі мен қимылдарын оқуға және біреудің қызығушылығын жоғалтып жатқанын немесе оны дауыстап айтпай-ақ ештеңеге үзілді-кесілді келіспейтінін түсінуге көмектеседі.

Команда әр түрлі елдерде спутниктік мобильді телефондарды байланыс арнасымен байланысқа шықты және семинар барысында халықаралық сапарларға шектеулер болғандықтан, қатысушылармен жеке кездесу мүмкін болмады. Семинарды онлайн-конференция форматында ұйымдастыру туралы шешім қабылданды.

Талқылау.

Семинар екі бөлімге бөлінді. Бірінші бөлім ақпараттық телекоммуникалау жүйесінің күтілетін қауіп-қатерді модельдеу семинарының кіріспе презентациясы болды. Қауіп-қатердің әдісі, процесі, ережелері мен субъектілері ұсынылған. Содан кейін жүйенің схемасына шолу және жүйеге қысқаша кіріспе жасалды.

Кіріспе презентациядан кейін жүйенің деректер ағынының схемасы экранды бөлісу арқылы ұсынылды және оны өнім менеджері түсіндірді.

Семинарда мобильді телефондардың байланыс арнасын қорғау әдістерін анықтау үшін қауіп-қатерді модельдеу тәжірибесі бар кейбір қатысушылар түрлі тәсілдерді ұсынды. Спутниктік мобильді телефондарды байланыс арнасының қорғау әлемдік

мәселелердің бірі екендігін көруге болады. Әртараптан жана идеялар да ұсынылып атап айтылыпта жатты.

Семинардың соңында ақпараттық телекоммуникалық жүйелердің қателерді сұрыптауға уақыт берілді және ұсыныстармен ой-пікірлер ұсынылды.

Семинарды бағалау

Семинар соңында семинардың негізгі қатысушыларымен құрылымсыз сұхбаттар өткізілді. Сонымен қатар, талдау Vaishnavi және мобильді телефондарды байланыс арнасының қорғау әдістері анықтау үшін басқалар ұсынған рефлексия мен абстракциямен жүргізілді. Жақсарту үшін бірнеше аймақ табылды. Олардың кейбіреулері дайындық кезеңіне, ал басқалары семинар кезеңіне жатады. 2-кестеде семинарға дайындықты жақсарту үшін бағалау және ұсынылған бағыттар бар.

2 кесте - Бағалау және жақсарту бағыттары-дайындық кезеңі

Элемент	Рейтинг	Қарастыру және жақсарту бойынша ұсыныстар
Шақырылғандар тізімі	Семинарға шақырылған адамдардың саны мен дағдыларының жиынтығы теорияға сәйкес келді. Басшылық шамадан тыс ұсынылды.	Мобильді телефондарды байланыс арнасының қорғау әдістерін анықтау үшін қауіп-қатерді анықтаудың шығармашылық кезеңінде басшылықтың болуы кейбір қызметкерлердің сөйлеуіне кедергі келтіруі мүмкін. Нұсқаулықтың болуы басымдықтар мен азайту стратегиялары туралы шешім қабылдау қажет болған кезде қателерді сұрыптау кезеңінде пайдалы.
Күн тәртібіне шақыру	Жұмыс сәтті аяқталды.	Қысқаша анықтамалық материалды және кішігірім жеке тапсырмаларды пайдалану қатысушылардың дайындық кезінде күш-жігерін жақсырақ бағыттауы мүмкін.
Формат	Онлайн семинар форматы миға шабуыл жасау үшін өте қолайлы болмады. Мүшелерді ұстау қиын. Дене тілі мен вербалды емес қарым-қатынасты оқу қиын. Мүмкіндігінше миға шабуыл бойынша онлайн семинарлардан аулақ болу керек.	Мобильді телефондарды байланыс арнасын қолдануда жүйеде салмақ түсті, қатысушылардың санын азайту керектігі анықталды. Дауыстық байланыс пен бейне байланысты қатар қамтамасыз ету қиындықтарын тұғызды. Семинарда веб-камераны пайдалану міндетті болуы керек еді. Белсенді қатысу үшін мотивациялық құралдарды қарастырылды. Мысалы, геймификация.
Онлайн конференция платформасы	MSTeams осы мақсатта жақсы қызмет етті.	Жергілікті аппаратар мен мобильды қозғалмалы аппараттарды қатар пайдаланғанда ең жақсы тәжірибелері платформаны қолдануға болатындығы зерттелді. Онлайн конференция құралдарында қол жетімді мүмкіндіктер тез дамып келеді, сондықтан оларды үнемі зерттеп, тәжірибе жасау ұсынылады.

Онлайн сурет салу құралы	Draw.io қанағаттанарлық болды.	Қарастырылатын негізгі мәселелер: аппараттық құрал бұлтты немесе офлайн ма; мобильді обьектілерме; онлайн ынтымақтастықты қолдайды ма, жоқ па; спутниктік және интернет арналарының жұмыс тиімділігін артырама; қауіп-қатерді модельдеу диаграммаларының кітапханасы бар ма, жоқ па? Қоғамдағы ақпараттық телекомммуникалық жүйелерді қолданудағы баға шешімдеріне де әсер етуі мүмкін.
Құрылымы және ұзақтығы	Ұзақтығы ақылға қонымды болды. Құрылымды қайта қарау керек.	Семинар шығармашылық және ақпараттық қауіптерді зерттеуге немесе тиімді шешім қабылдау арқылы қауіп қателерді талдауға бағытталуы мүмкін. Гибридті жағдайлар дұрыс жұмыс істемеуі мүмкіншіліктерінің сапасын артыру жағдайлары берілуі мүмкін.
Диаграмма жасау	Кездесу уақытын үнемдеу үшін жүйенің деректер ағынының схемасын алдын ала жасаңыз. Алайда, бұл карталармен бірлесіп жұмыс істеудің оң әсерін азайтты.	Семинар ағымындағы деректер ағынының диаграммасын бірге құру топ үшін мұзды ерітуге және жүйенің жалпы түсінігін жақсартуға көмектесетін жақсы құрал бола алады. Сонымен қатар, бұл барлығына қиындықтарды немесе басымдықтарды анықтауға көмектеседі.

Ақпараттық телекоммуникациялық жүйлердің талдануы мен зерттелуі дайындық кезеңінің негізгі қорытындысы - кездесудің мақсатына дұрыс команданы жинау және мақсаттар мен үміттерді нақты тұжырымдау өте маңызды [10]. Сонымен қатар, әрбір қорытынды үшін қайта қарау және жақсарту бойынша ұсыныстар 3-кестеде берілген [11].

3 кесте - Бағалау және жақсарту бағыттары-семинар кезеңі

Элемент	Рейтингі	Қарастыру және жақсарту бойынша ұсыныстар
Кіріспе презентация	Жұмыс сәтті аяқталды.	Команда байланыс құралдары мен байланыс арналарының қауіп-қатерді модельдеуде неғұрлым тәжірибелі болса, кіріспе презентацияға соғұрлым аз уақыт кетеді. Осы кезде әр қатысушыдан отыз секундтық кіріспе беру, олардың рөлі, үміттері және семинарға қосқан үлесі туралы айту сұралуы керек. Бұл сеанс кезінде белсенді қатысу деңгейін жоғарылатуы мүмкін.
Жүйе схемасының тұсаукесері	Түсініктеме жақсы болды, бірақ орташа әсер етті.	Жүйенің сипаттамасы жақсы жасалғанымен, шектеулі әсерлері мен болашақта зерттеулерді талап ететіндігі айтылды.

Миға шабуыл	Бұл аралас нәтижелерге ие болды.	Жоғарыда сипатталғандай, онлайн платформа арқылы гибриттік байланысты жасау қиын міндеттер екендігі анықталды. Оның нәтижесіне көптеген факторлар әсер етуі мүмкін, мысалы, мәдени ерекшеліктер, корпоративті мәдениет, бұлттық технологиялар мен мобильді байланыс құралдарының бір-бірімен байланыстарын насихатайтын қатысулар, көшбасшылар қатысуы. Мұны ескеру қажет.
Әдіс	Әрбір элемент үшін таңдалған STRIDE әдісі онлайн ми шабуылы кезінде жұмыс істемеді.	Егер қатысушылар арасында қауіп-қатерді модельдеу тәжірибесі бар адамдар болса, семинар алдында олармен алдын-ала итерация жасалды. Бұл әркімнің әдіспен келісетінін растауға көмек береді..
Веб-камераны пайдалану	Жұмыс сәтсіз аяқталды.	Егер адамдар веб-камераларын өшіруді шешсе, бұл мінез-құлықты өзгерту үшін тиісті мотивациялық құралдарды қарастырған жөн.
Техникалық инфрақұрылым (интернет, микрофон, шешен)	Интернетке жоғары жылдамдықты қол жетімділіктің кең таралуына қарамастан, байланыс кейде үзіліп қалады. Динамиктер мен микрофондар пайдаланушы тәжірибесіне қатты әсер етті.	Интернеттегі ми шабуылының тағы бір кемшілігі-күтпеген оқиғалар болуы мүмкін. Мобильды телефондар мен электронды есептеу машинарларындағы қатысушы мүшелер қосыла алмайды, интернет байланысы тұрақсыз болуы мүмкін немесе интернет байланыс арнасының әлсіздігі, аппараттық кемшіліктер- біреудің динамиктері жаңғырық тудыруы мүмкін. Семинарда көптеген адамдарды әлемнің әр түрлі орындарнан бір платформада қосу кейбір қиындықтарды тудырды және алдын алу немесе жоспарлау қиындық тудырды.

Семинар кезеңінде ақпараттық телекоммуникалық жүйлердің әртүрлі технологиялары зерттелді, топпен жұмыс жасалды [12]. Жоғарыда талқыланғандай, гибридті байланыста дауыстық және бейне байланысты қатар ұстау, веб-камераны үнемі пайдалану сияқты мәдениет пен корпоративтік мәдениет мәселесі туындады.

Қорытынды.

Бұл мақалада спутниктік байланыс арналары мен жердегі сегменттер және ақпараттық телекоммуникалық жүйлердің ақпараттық қауіпсіздік қатерлерін модельдеу қарастырылады. Қауіп-қатерді модельдеуге, оның ішінде жердегі спутниктік жүйелерді қорғауға теориялық талдау жасалды. Қоғамдағы бқлттық технология мен мобильді обьектілер және мобильді телефондардың байланыс арналарын тиімді қорғау әдістерін анықтау үшін, болашақтағы қауып қатерлерді алын алу үшін семинар өткізілді және пікірлер мен ұсыныстар талданды. Практикалық бөлімде жер сегментіне қауіп-қатерді модельдеу, спутниктік байланыс арналарының қауіп-қатерді модельдеу бойынша семинарды ұйымдастыру және бағалау сипатталған.

Осы мақалада спутниктік мобильді обьектілер мен мобильді телефондардың арналары мен оларды іске асыратын аппаратуралардың арасындағы деректер

байнанысының киберқауіпсіздік қауіптерін талдау және бағдарламалық қорғау ықтималдық мәселелері зерттелді.

Алғыс білдіру. Бұл жұмысты Қазақстан Республикасы Ғылым және жоғары білім министрлігінің Ғылым комитеті қаржылай қолдады (№ BR18574045).

ӘДЕБИЕТТЕР

[1] Манулис М, Бриджес СП, Харрисон Р, Секар В., Дэвис А. Жаңа кеңістіктегі киберқауіпсіздік: қауіптерді, негізгі технологиялар мен мәселелерді талдау, Суррей киберқауіпсіздік орталығы, Суррей университеті, Гилфорд, Ұлыбритания, 2022 ж.

[2] Tom Sarafin, Poti Doukas, Lenny Demchak and Mike Browning, "Vibration Testing of Small Satellites", Rev B, July 2017. [Online]. Available:Instar, http://instarengineering.com/vibration_testing_of_small_satellites.html [Accessed August 15, 2018].

[3] Манулис М. және басқалар жаңа кеңістіктегі киберқауіпсіздік // Халықаралық ақпараттық қауіпсіздік журналы (2021) 20: 287-311 б.

[4] Молдамурат К., Өтеген А. С., Бримжанова С. С., Қалманова Д. М., Ыскелди н. Г. Шағын спутниктер тобын басқаруға арналған бағдарламалық тренажер әзірлеу // 2021 Электроника, компьютерлер және есептеу бойынша халықаралық конференциясы // ICECCO-Conference Paper-2021.

[5] Хиллеви Н, Линнеа П. Швецияның Ғарыш саласындағы киберқауіпсіздікті пәнаралық талдау // Упсала университеті – 2022.

[6] Бела Б-П. Ғарыш саласындағы киберқауіпсіздік // JAMK-2021 Қолданбалы ғылымдар университеті.

[7] ISO 15864:2021 Space systems – General test methods for spacecraft, subsystems and units.

[8] Gecha V.Ya., Kanunnikova E.A., Pugach I.Yu. Computational and experimental study of dynamic characteristics of spacecraft // Reliability. -M. - 2008 № 4. - pp. 37-41.

[9] Джеймс П. Жаңа кеңістіктің қауіпсіздігін қамтамасыз ету: спутниктік киберқауіпсіздік // Вольфсон – Хилари колледжі, 2021 ж.

[10] Kanunnikova E.A., Pugach I.Yu. Computational and experimental study of dynamic characteristics of antenna devices of spacecraft // Questions of Electromechanics. Proceedings of NPP VNIIEM. - M.: FSUE "NPP VNIIEM", 2009. - Vol. 109. - pp. 17-20

[11] Кереев А. К., Атанов С.К., Аман К. П., Құлмағамбетова З. К., Құлжағарова Б. Т. Bluetooth-маяктарға негізделген навигациялық жүйе: іске асыру және эксперименттік бағалау // Теориялық және қолданбалы ақпараттық технологиялар журналы. – Мақала. 2020, 98 (8), 1187-1200 б.

[12] Мельничук А., Кузина Е. А., Юрков Н. К. Ұшқышсыз ұшу аппараттарына қарсы іс – қимыл әдістері мен құралдары // Өнеркәсіптік инжиниринг, қосымшалар және өндіріс бойынша халықаралық конференция, ICIEAM 2020-Конференция баяндамасы. – 2020, 9112082.

REFERENCES*

[1] Manulis M, Bridzhes SP, Harrison R, Sekar V., Djevis A. Zhana kenistikteki kiberkauipsizdik: kauipterdi, nekizki tehnolokijalar men maselelerdi taldau, Surrej kiberkauipsizdik ortalygy, Surrej universiteti, Kilford, Ulybritanija, 2022 zh.

[3] Manulis M. zhane baskalar zhana kenistikteki kiberkauipsizdik // Halykaralyk akparattyk kauipsizdik zhurnaly (2021) 20: 287-311 b.

[4] Moldamurat K., Oteken A. S., Brimzhanova S. S., Kalmanova D. M., Yyskeldi n. K. Shagyn sputnikter tobyn baskaruga arnalgan bagdarlamalyk trenazher azirleu // 2021 Jelektronika, komp'juterler zhane esepteu bojynsha halykaralyk konferencijasy // ICECCO-Conference Paper-2021.

[5] Hillevi N, Linnea P. Shvecijanyn Garysh salasyndagy kiberkauipsizdikti panaralyk taldau // Upsala universiteti – 2022.

[6] Bela B-P. Garysh salasyndagy kiberkauipsizdik // JAMK-2021 Koldanbaly gylymdar universiteti.

[9] Dzhejms P. Zhana kenistiktin kauipsizdikin kamtamasyz etu: sputniktik kiberkauipsizdik // Vol'fson – Hilari kolledzhi, 2021 zh.

[11] Kereev A. K., Atanov S.K., Aman K. P., Kulmagambetova Z. K., Kulzhagarova B. T. Bluetooth-majaktarga nekizdelken navikacijalyk zhyje: iske asyru zhane jeksperimenttik bagalau // Teorijalyk zhane koldanbaly akparattyk tehnolokijalar zhurnaly – Makala. 2020, 98 (8), 1187-1200 b.

[12] Mel'nichuk A., Kuzina E. A., Jurkov N. K. Ushkyshsyz ushu apparattaryna karsy is – kimyl adisteri men kuraldary // Onerkasiptik inzhinirink, kosymshalar zhane ondiris bojynsha halykaralyk konferencija, ICIEAM 2020-Konferencija bajandamasy. – 2020, 9112082.

Mahabbat Bakyt, doctoral student, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, makhabbat@gmail.com

Huralai Moldamurat, candidate of technical sciences, docent, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, moldamurat@yandex.kz

Yerzhan Seytkulov, candidate of physical and mathematical sciences, professor, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, yerzhan.seitkulov@gmail.com

Sabyrzhan Atanov, doctor of technical sciences, professor, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, atanov5@mail.ru

Mahsut Bekenov, candidate of physical and mathematical sciences, professor, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, moldamurat@yandex.kz

CYBERSECURITY THREAT ANALYSIS FOR SATELLITE MOBILE PHONE DATA

Annotation. This article examines the issues of analysis of cybersecurity threats and software protection for satellite mobile objects and mobile phone channels, data in the equipment that implements them. Technologies and effective approaches to application in the information and telecommunication system are considered. Analysis of cybersecurity threats to low-orbit aircraft data. Satellite cybersecurity is an important topic today. Contributions were divided by disciplines ranging from history and security studies to aerospace engineering and astrophysics. This article attempts to highlight these interdisciplinary contributions and systematize knowledge about the security status of space systems. The system begins with modeling information security threats for the ground segment of space communications. Threats to space systems are described in a single matrix linking attackers, vulnerabilities and motives. This model is confirmed by the full historical time of satellite events. The end result is an empirical and proven foundation for those who advocate space system safety research. A theoretical analysis of threat modeling, including the protection of low-orbit aircraft, will be carried out. The article also describes threat modeling for low-orbit aircraft data, organization and evaluation of a threat modeling workshop.

Keywords. Satellite mobile objects, cybersecurity of mobile phones, space communication channels, information security, encryption, information telecommunications system, low-orbit aircraft.

Махаббат Бақыт, докторант, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан, makhabbat@gmail.com

Хуралай Молдамурат, к.т.н., доцент, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан, moldamurat@yandex.kz

Ержан Сейтқұлов, к.ф.-м.н., профессор, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан, yerzhan.seitkulov@gmail.com

Сабыржан Атанов, д.т.н., профессор, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан, atanov5@mail.ru

Махсут Бекенов, к.ф.-м.н., профессор, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан, moldamurat@yandex.kz

АНАЛИЗ УГРОЗ КИБЕРБЕЗОПАСНОСТИ ДЛЯ ДАННЫХ СПУТНИКОВЫХ МОБИЛЬНЫХ ТЕЛЕФОНОВ

Аннотация. В данной статье исследованы вопросы анализа угроз кибербезопасности и программной защиты для спутниковых мобильных объектов и каналов мобильных телефонов, данных в аппаратуре, их реализующей. Рассмотрены технологии и эффективные подходы к применению в информационно-телекоммуникационной системе. Анализ угроз кибербезопасности для данных низкоорбитальных летательных аппаратов. Сегодня спутниковая кибербезопасность является важной темой. Взносы были разделены по дисциплинам, начиная от истории и исследований безопасности и заканчивая аэрокосмической инженерией и астрофизикой. В этой статье делается попытка выделить эти междисциплинарные вклады и систематизировать знания о статусе безопасности космических систем. Система начинается с моделирования угроз информационной безопасности для наземного сегмента космической связи. Угрозы космическим системам описываются в единой матрице, связывающей злоумышленников, уязвимости и мотивы. Эта модель подтверждается полным историческим временем спутниковых событий. Конечным результатом является эмпирическая и доказанная основа для тех, кто выступает за исследования безопасности космических систем. Будет проведен теоретический анализ моделирования угроз, включая защиту низкоорбитальных самолетов. В статье также описывает моделирование угроз для данных низкоорбитальных летательных аппаратов, организацию и оценку семинара по моделированию угроз.

Ключевые слова. Спутниковые мобильные объекты, кибербезопасность мобильных телефонов, космические каналы связи, информационная безопасность, шифрование, информационная телекоммуникационная система, низкоорбитальные летательные аппараты.

****