



Студенттер мен жас ғалымдардың
«ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2018»
XIII Халықаралық ғылыми конференциясы

СБОРНИК МАТЕРИАЛОВ

XIII Международная научная конференция
студентов и молодых ученых
«НАУКА И ОБРАЗОВАНИЕ - 2018»

The XIII International Scientific Conference
for Students and Young Scientists
«SCIENCE AND EDUCATION - 2018»



12th April 2018, Astana

**ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ**

**Студенттер мен жас ғалымдардың
«Ғылым және білім - 2018»
атты XIII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ**

**СБОРНИК МАТЕРИАЛОВ
XIII Международной научной конференции
студентов и молодых ученых
«Наука и образование - 2018»**

**PROCEEDINGS
of the XIII International Scientific Conference
for students and young scholars
«Science and education - 2018»**

2018 жыл 12 сәуір

Астана

УДК 378

ББК 74.58

Ғ 96

Ғ 96

«Ғылым және білім – 2018» атты студенттер мен жас ғалымдардың XIII Халықаралық ғылыми конференциясы = XIII Международная научная конференция студентов и молодых ученых «Наука и образование - 2018» = The XIII International Scientific Conference for students and young scholars «Science and education - 2018». – Астана: <http://www.eni.kz/ru/nauka/nauka-i-obrazovanie/>, 2018. – 7513 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-997-6

Жинаққа студенттердің, магистранттардың, докторанттардың 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.

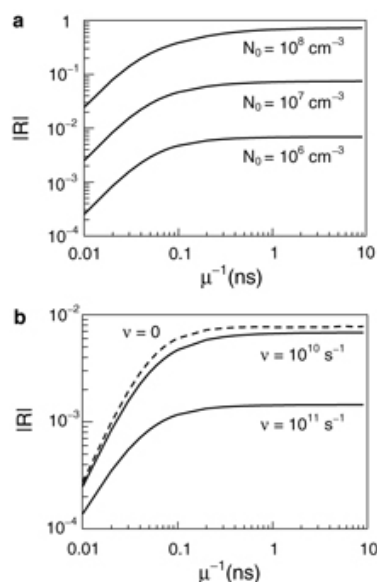
В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 378

ББК 74.58

ISBN 978-9965-31-997-6

©Л.Н. Гумилев атындағы Еуразия
ұлттық университеті, 2018



Сурет 2 – Көріну коэффициентінің абсолютті мәні

2-суретте коэффициентінің абсолютті мәні көрсетілген $|R| = |E_r|/|E_0|$ $\mu = 30$, $\theta_0 = 45^\circ$ плазма өмір сүру ұзақтығының функциясы ретінде және әртүрлі N_0 және ν . Тәуелділік $|R(\mu^{-1})|$ өте тез $\mu^{-1} \sim 1$ нс кезінде қаныққан. Төменгі $\gamma = 10$ кезінде қанықтыру $\mu^{-1} \sim 10$ нс кезінде (көрсетілмеді) баяу орындалады. Бір қызығы, үшін $\omega_0/(2\pi) = 10$ МГц үшін қарастырылған жағдайда қанықтыру $|R(\mu^{-1})|$ мәндерінде шамамен он есе аз болатын: $\gamma = 30$ және 10 үшін 0,1 және 1 нс.

Қолданылған әдебиеттер тізімі

1. Gary S. Sales, OTH-B radar system: System summary. // 56
2. Петров В. Современное состояние и перспективы развития загоризонтных радиолокационных станций зарубежных стран // Зарубежное военное обозрение № 10 2008 С.27-31
3. D.H. Sinnott. The Development of Over-the-Horizon Radar in Australia.
4. Давыдов Ю. К истории загоризонтной радиолокации. Воздушно-космическая оборона. 2013.

ӘОЖ 629.78

СПУТНИКТІК БАЙЛАНЫС АРҚЫЛЫ ДЕРЕКТЕР АЛМАСУДА АҚПАРАТТЫ ҚОРҒАУ

¹Саясат Нұрбакытбек Жеткіншекұлы, ²Мұстафаева Әсел Нұрланқызы, ³Рыскелды Назерке Ғазизқызы

¹Л. Н. Гумилев атындағы ЕҰУ «Ғарыштық техника және технологиялар»
кафедрасының 3 курс студенті, Астана, Қазақстан

^{2,3}Л. Н. Гумилев атындағы ЕҰУ «Ғарыштық техника және технологиялар»
кафедрасының лаборанты, Астана, Қазақстан
Ғылыми-жетекші – Х.Молдамурат

Бұл мақалада спутниктік байланыс арқылы деректер алмасуда ақпаратты қорғаудың әдісі берілген. Осы әдістің негізінде RSA арқылы шифрленген қорғалған хаттама көрсетілген. Сондай-ақ Хемминг кодының басты артықшылығы айқындалды.

Түйінді сөздер: спутниктік байланыс, криптография, ақпарат алмасу, қорғалған хаттама.

Ғылыми-техникалық саладағы жетістіктер қарулы қатығыс технологияларының дамуына айтарлықтай әсер етеді. Қазіргі кезде бірқатар елдердің әскери бөлімдері сетецентрикалық соғыс технологиясын дамытып келеді. Сетецентрикалық соғыстың басты мазмұны оның жеке ақпараттық технологияларына тән ақпараттық артықшылықтарды аударуы болып табылады. Нақты артықшылығы ақпаратты қамтамасыздандырылған, географиялық тұрақталған күштердің тұрақты желіге бірігуінде. Бұл жедел, тактикалық, әрі стратегиялық сынды әскери операциялардың барлық деңгейлерінде жүргізе алады. Қазіргі уақытта деректерді (басқару пәрмендерді) жіберу үшін спутниктік байланыс жиі пайдаланылады. Мұндай байланыс түрін пайдалану барлық деректердің қорғалмаған байланыс арнасы арқылы берілуін білдіреді, яғни мұндай жүйелер «ортасында адам бар» деп аталатын осалдықты тудырады. Осылайша, деректерді ұстап қалу немесе басқа деректерді енгізу мүмкіндігін болдырмау үшін байланыс арнасын қорғау жөніндегі шараларды қабылдау қажет. Ақпараттың тұтастығын және құпиялылығын, сондай-ақ қолжетімділігін қамтамасыз ету керек.

Әскери операцияларды дайындау мен өткізудің жаңа технологияларына тиісті әртүрлі тактикалық әдістер мен әскердің, сондай-ақ жау әскерлерінің күшті және әлсіз жақтарын ескере отырып, әскери техника мен қаруландыру технологиясын қарама-қарсы қою керек.

Бұл жұмыстың мақсаты – ақпаратты қорғауды жүзеге асырудың ықтимал әдісін ұсыну болып табылады.

Жиі желіаралық экрандар интернет желісінің бірнеше сегменттері арасында қауіпсіз арнасын жасау үшін пайдаланылады. Бұл функция өте ыңғайлы, себебі корпоративтік мақсаттарда Интернеттің мүмкіндіктерін өте тиімді пайдалануға мүмкіндік береді. Осындай арналарды құру үшін арнайы ақпаратты шифрлеу хаттамалары қолданылады. Бұл жағдайда жеткілікті жылдам шифрлау алгоритмін пайдалану қажет, себебі берілетін ақпарат көлемі үлкен болуы мүмкін және баяу шифрлау алгоритмдері хабар алмасуды қиындатады. Ашық кілтті шифрлеу алгоритмдері әдетте баяу жұмыс жасайды, сондықтан ақпараттың үлкен ағынын шифрлеуде бірдей құпия кілтті қолданатын шифрлеу мен дешифрлеу алгоритмы пайдаланады.

Симметриялы шифрлауды пайдаланудың күрделілігі - хабарлардың жіберушісі мен қабылдағышы бірдей құпия кілтті білуі керек. Бұл дегеніміз, мұндай кілтті желі арқылы шифрлемей жіберуге болмайды. Бірақ жіберу керек. Бұл мәселенің ең перспективалы шешімі - құпия кілттерді асимметриялық алгоритмде шифрлау және хабардың негізгі мәтіні құпия кілттерді қолданумен симметриялы болып табылады. Сонымен қатар, ашық кілттер алгоритмін пайдаланып хабарларды беру үшін сертификаттардың дамыған жүйесі қажет. Бұл жағдайда сертификат пайдаланушылары туралы емес, сонымен қатар тыңдаудан қорғалған қосылыс компьютерлері туралы сертификаттар туралы болуы мүмкін.

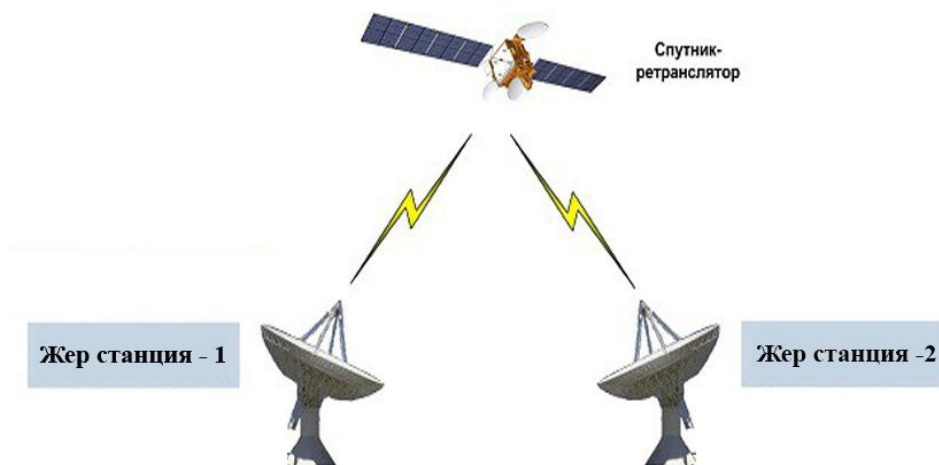
Әлі күнге дейін тек желінің берілуінде жалғыз хабарлардың қорғалуы қарастырылған, бірақ әдетте көп уақыт ішінде желі субъектілері арасында көптеген хабарлар жіберіледі.

Негізгі шифрлау кілті хабарларды беру үшін қайта пайдаланылады. Бұл шабуылдаушыға хабарларды кешіктіруге, жоюға, ауыстыруға немесе қайталауға мүмкіндік береді. Хабар деңгейіндегі түпнұсқалығын растау осындай әрекеттерден қорғауды қамтамасыз етпейді, себебі хабар өзі өзгермейді. Дегенмен, мұндай енулерден қорғаудың әр түрлі әдістері бар.

Сымсыз спутникалық арнадағы деректердің қауіпсіздігін қамтамасыз етудің басты жолы аппараттық-бағдарламалық құралдарды пайдалануда. Біріншіден, сыртқы желілермен барлық ақпарат алмасу берілген қауіпсіздік саясатына сәйкес шекаралық маршрутизаторлар мен оператордың желіаралық экранында бақыланады. Екіншіден, берілген деректер спутниктік жабдықтарды өндірушінің шифрлау алгоритмдеріне сәйкес шифрленеді. Үшіншіден, желі мен серверлердің жұмысы туралы үнемі статистиканы жинау, техникалық

қызметтің желі жұмысын кез келген уақытта тиімді бақылауға және түзетуге мүмкіндігін береді.

Төменде жердегі станция, спутник-ретранслятор, жердегі станция типтегі схема бойынша ақпарат беруде ақпаратты қорғау әдісі беріледі. Бұл сызба төмендегі суретте көрсетілген.



Сурет 1 – Деректерді беру схемасы

Қорғау әдісі ретінде, мәтіндік хабарларды, мысалы, кез келген командаларды берудің сенімді хаттамасын қолдану ұсынылады. Хаттаманың орындалуын тексеру үшін оның орындалуы көрсетілетін бағдарлама жасалынған. Бұл бағдарлама TCP протоколын абстракталандыру арқылы шифрленген мәтіндік хабарламаларды жіберуге және оларды дешифрлеуге мүмкіндік береді. Деректер RSA шифрлау алгоритмі арқылы шифрленеді. Бұл алгоритм іске асу оңай болғандықтан таңдалды.

Пайдаланушы клиенттің немесе сервердің рөлін таңдай алады. Сервер рөлін таңдаса, клиент қосылатын портты және кілт өлшемін (256, 512, 1024, 2048 биттер) көрсете алады.

Егер клиент рөлі таңдалған болса, сервердің IP мекенжайын және портын енгізу қажет болады.

Криптографиялық хаттаманы тексеру кезінде дешифрлеудегі ешқандай қате табылмады. Хабарламаларды жіберу және қабылдау жылдамдығына байланысты шамалы кемшіліктер табылды. Әр жаңа хабарды жібермес бұрын жаңа кілттердің жұбын жасау төмен жылдамдықты туғызды.

Бұл бағдарлама интернет байланысын қажет етеді. Портты көрсетуде алдын-ала келісу керек. Бағдарламаның өзі портты ашу туралы өтініш жасамайды, бұл үшінші тараптың қосылымдарынан қорғау үшін қолданылады. Егер үшінші тарап сервер тыңдайтын портты білмесе, онда ол бірінші порт туралы білуі керек.

Спутниктік байланыс жағдайында деректерді ғарыш аппаратына ашық арна арқылы берілетінін ескеру қажет. Сондай-ақ деректерді жіберу кезінде қате болуы мүмкін екенін ескеру керек. Қателерді анықтау үшін Хемминг кодын қолдану ұсынылады.

Хемминг коды тамаша кодтардың класына жатады, яғни кез келген бірқатарлы қатені түзетеді, бірақ ол жоғары сан алуан бірнеше қатарлы қателерді түзете алмайды. Дегенмен ол бір және екі қатарлы қателерді анықтай алады. Сондықтан, қателер анықталған кезде кодты комбинацияда бірқатарлы қате пайда болды деген болжамдармен қосымша декодтау орындалады.

Бұл бағдарлама деректерді қорғау және «ортадағы адамның» шабуылын алдын алу үшін әзірленген хаттаманың ерекшелігін жүзеге асыру болып табылады. Хаттаманың сипаттамасына Хемминг кодын қосу және оны іске асыру арқылы оның кеңейтілген деректерінің жұмыс істеу қабілеттілігін тексеру үшін функция құру жоспарлануда.

Аппараттық және бағдарламалық қамтамасыз етуден басқа, спутниктік операторлар байланыс түйіндерін қорғау үшін ұйымдастырушылық және әкімшілік шаралардың кешенін пайдаланады.

Қауіпсіздік шараларының толық спектрімен қоса пайдаланушылар әлемдегі ең қауіпсіз телекоммуникациялық шешімдердің бірін алады, бұл ақпараттың құпиялылығы үшін ең жоғары талаптарға жауап береді. Спутниктік жүйелер икемді түрде конфигурацияланған, ол жоғары технологиялық өндірістерде жұмыс істейтін клиенттердің өсіп келе жатқан сұранысына бейімделуге мүмкіндік береді. Мәселен, мұнай-газ компаниялары үшін спутниктік байланыс бүгінгі күні де-факто стандарты болып саналады. Бұл спутниктік технологияның пайдасына маңызды дәлел.

Осылайша, спутниктік байланыс арқылы берілетін деректерді қорғау тәсілдерінің бірі схемаға сәйкес жүзеге асырылды: жердегі станция, спутниктік ретранслятор, жер станциясы.

Қолданылған әдебиеттер тізімі

1. Немировского А. С. Радиорелейные и спутниковые системы передачи : учебник для вузов. М. : Радио и связь, 1986. С. 192.
2. Акулиничев Ю. П. Теория электрической связи : учеб, пособие. СПб. : Лань, 2010. С. 87.
3. Малюк А. А. Теория защиты информации. — М.:Горячая линия — Телеком, 2012. — 184 с. — ISBN 978-5-9912-0246-6.
4. Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты. СПб.: Питер, 2008. — 272 с. — ISBN 978-5-388-00069-9.
5. Петренко С.А., Курбатов В.А. Политики информационной безопасности. — М.: Компания АйТи, 2006. — 400 с. — ISBN 5-98453-024.
6. Галатенко В. А. Стандарты информационной безопасности. — М.: Интернет-университет информационных технологий, 2006. — 264 с. — ISBN 5-9556-0053-1.
7. Галицкий А. В., Рябко С. Д., Шаньгин В. Ф. Защита информации в сети — анализ технологий и синтез решений. М.: ДМК Пресс, 2004. — 616 с. — ISBN 5-94074-244-0.

УДК 629.78

МИКРОПРОЦЕССОРЫ ДЛЯ КОСМИЧЕСКИХ ПРИМЕНЕНИЙ

Султанов Дияс Нуржанович

Студент кафедры космической техники и технологии

ЕНУ им. Л.Н.Гумилева, Астана, Казахстан

Научный руководитель – Алдыярова Б.Т.

Введение. Эксплуатация интегральных схем (ИС) и микропроцессоров, в частности, на борту космического аппарата, характеризуются наличием радиационных факторов космического пространства, воздействующих на интегральные схемы и меняющие их свойства, вплоть до вывода их из работоспособного состояния. Источником радиационного воздействия являются потоки заряженных частиц — электронов, высокоэнергетических протонов (ВЭП) и ионов различных элементов, вплоть до урана, называемых также тяжелыми заряженными частицами (ТЗЧ). По своему происхождению, частицы разделяются на протоны и электроны естественных радиационных полей Земли (ЕРПЗ); протоны и ионы от Солнца, т.н. солнечные космические лучи (СКЛ); протоны и ионы из внешнего космического пространства, т.н. галактические космические лучи (ГКЛ). Воздействие потоков заряженных частиц на элементы ИС может вызвать следующие эффекты:

1. Эффекты полной поглощенной дозы (Total Ionizing Dose, TID), выражающиеся в том, что проходящие сквозь кремний микросхемы заряженные частицы вызывают