реалізується за допомогою перетворень даної інформації з використанням спеціальних даних (ключових) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства. Використання криптографічного захисту інформації під час побудови політики безпеки on-line-сервісу значно посилює безпеку роботи системи, але за умови, що ця система захисту створена належним чином та має безпечну систему розподілу криптографічних ключів.

41. БЕЗОПАСНОСТЬ M2M/ЮТ СИСТЕМ И ТЕХНОЛОГИИ BLOCKCHAIN

к.т.н., доц. Смидович Л.С., к.т.н., доц. Кулик Ю.А., НАУ "ХАИ", Харьков.

Одной из важных задач при разработке и внедрении M2M/IoT систем является обеспечение их безопасности, особенно в таких сферах, как управление производством и инфраструктурой, здравоохранение и т.п. В стандартах ETSI предлагается рассматривать M2M/IoT систему как многоуровневую, состоящую в частности из M2M/IoT устройств, шлюзов, приложений и серверов управления. Управление безопасностью, в том числе идентификация, авторизация и аутентификация, в данном случае выполняется централизованно, что потенциально может являться точкой отказа системы. Альтернативой может быть применение технологии blockchain. В этом случае все информационные и управляющие запросы в M2M/IoT системе рассматриваются как транзакции, а blockchain выступает в качестве распределённой, защищённой и прозрачной базы данных для их хранения. Это позволяет решить такие проблемы, как наличие единой точки отказа, защитить данные от злонамеренного изменения и компрометации.

42. ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ DMVPN ДЛЯ ЗАХИСТУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

к.т.н., с.н.с. Волошко С.В., Черницька І.О., Варига Н.Г., ПНТУ, Полтава

Актуальність проблеми інформаційної безпеки визначається рядом взаємозв'язаних факторів, більшість з яких є наслідком процесу інформатизації сучасного суспільства. Однак, використання інформаційних технологій приховує в собі значні ризики, які потрібно постійно відстежувати та враховувати. Фактично, дані ризики призводять до втрати конфіденційності, цілісності й доступності інформації, тобто, до порушення інформаційної безпеки. Різке зростання масштабів і складності інформаційно-телекомунікаційних мереж та збільшення кількості інформації, що в них циркулює, призводить до збільшення загроз інформації (як випадкових, так і умисних) і збитків від них. Цей факт вимагає впровадження нових технологій для захищеної передачі даних в мережах. У доповіді проведений аналіз процесу захищеної передачі інформації в інформаційно-телекомунікаційній мережі, протоколів віртуальних приватних мереж, обгрунтовано необхідність застосування DMVPN в інформаційно-телекомунікаційних мережах.

ПІДСЕКЦІЯ 1.3. ЗАСТОСУВАННЯ ТА ЕКСПЛУАТАЦІЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

1. INCREASING OF SATELLITE TELECOMMUNICATION SYSTEMS EXPLOITATION NOISE IMMUNITY ON THE AREA OF SPACE CRAFT'S NEAR-EARTH ORBIT INJECTION

Ph.D., ass. prof. Shefer O., Poltava National technical Yuri Kondratyuk University, Poltava

The ways of improving the reliability of telemetry with the spacecraft (SC) during its passage to the ionospheric flight area was examined in this article. The problem with radio waves propagation was arisen as a result of plasma shell formation around the SC. As a consequence, electrons' density in the space has changed, and frequently-selective radio signals' fadings have occurred, thus, as a result, the communication reliability with SC reducing. For increasing noise-immunity and reliability of telemetry with SC one can use organizational, energy or signal meth-

ods, but they have some drawbacks from energy to economic one. A method of local influence on outer plasma shell was suggested with the purpose of its density reducing in the SC's antenna compartment. The possibilities of low-temperature artificial plasma utilizing as a source of its interaction with outer plasma have been investigated. High intensity of artificial plasma radiation combines with minimum energy consumptions on its creation. These studies have proved the presence of local channel with a reduced density that is proposed to use like an unobstructed path of communication signals' passage with SC.

2. АНАЛІЗ МОЖЛИВОСТІ ВИКОРИСТАННЯ МЕРЕЖОЦЕНТРИЧНОЇ МОДЕЛІ ПРИ ЗАСТОСУВАННІ ЗАСОБІВ УРАЖЕННЯ ПО ДАНИМ ОПТИКО-ЕЛЕКТРОННОГО СПОСТЕРЕЖЕННЯ

к.т.н., доц. Іващук Б.М., к.т.н. Кібіткін С.О., ХНУПС, Токатли М.В., НДПКТІ мікрографії, Харків

У доповіді приведено аналіз застосування засобів ураження по даним оптико-електронного спостереження (ОЕС) запомогою використання мережоцентричної моделі. Для успішного досягнення намічених цілей підрозділам та частинам збройних сил необхідна інформація про противника. Завдання по добування цієї інформації виконують засоби ОЕС. Якість інформації про об'єкти противника залежить від обладнання спостереження, що встановлено на пілотованих та безпілотних літальних апаратах (ЛА та БПЛА). За допомогою заміни аналогового обладнання спостереження на цифрове дозволить зменшити час за рахунок відсутності довготривалого процесу хімікофотографічної обробки. Також перехід на цифрові системи надасть можливість застосовувати нові моделі ведення спостереження такі як мережоцентрична модель виконання завдань. Використання мережоцентричної моделі у військовому сенсі — це застосування військ та зброї. Застосування цієї концепції значною мірою впливає на оперативність прийняття рішення. Концепція передбачає перетворення переваг окремих інфокомунікаційних технологій в конкурентну перевагу за рахунок об'єднання в стійку мережу інформаційно досить добре забезпечених та географічно розосереджених сил.

3. МОДЕЛЮВАННЯ МНОЖИННОГО ДОСТУПУ АБОНЕНТІВ ДО БЕЗДРОТОВОЇ КОМП`ЮТЕРНОЇ МЕРЕЖІ З КОДОВИМ РОЗПОДІЛЕННЯМ КАНАЛІВ

к.т.н., доц. Бердніков А.Г., магістрант Горбунов В.В., ХНУ, Харків

Однією з головних причин швидкого розвитку множинного доступу є висока ефективність методу, можливість побудови систем з вигідними експлуатаційними характеристиками. Завдання підвищення ефективності виробництва, а також забезпечення якості управління, контролю і передачі є насущними для будь-якого підприємства, особливо, якщо технологічні процеси складні і найменший збій може призвести до суттєвих економічних втрат. Сучасним інструментом для вирішення цих завдань є автоматизована система управління технологічними процесами - АСУ ТП. Складовими частинами АСУ ТП можуть бути окремі системи автоматичного управління та автоматизовані пристрої, пов'язані в єдиний комплекс. Предметом роботи є побудова моделі методів множинного доступу абонентів до бездротової комп`ютерної мережі з кодовим розподіленням каналів. На основі аналізу технологій множинного доступу з кодовим розподіленням каналів методом псевдовипадкової стрибкоподібної перебудови частоти (FHSS) і шляхом розширення спектра за допомогою прямої послідовності (DSSS) розроблені програмні моделі на базі поширених послідовностей. Проведено порівняння ефективності методів, показано підвищення завадостійкості інформаційного обміну за рахунок обчислення автокореляційної функції послідовності коду Баркера та підтверджено функціонування моделі технології DSSS, яка забезпечує синхронну передачу даних від датчиків до приймача центрального вузла, та забезпечує поділ сигналів, закодованих кодом Уолша.