НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ННК "Інститут прикладного системного аналізу"
(повна назва інституту/факультету)

Кафедра Системного проектування
(повна назва кафедри)

«До захисту допущено»

Завідувач кафедри
_____ А.І.Петренко
(підпис) (ініціали, прізвище)
"___"_____2015 р.

Дипломна робота

першого (бакалаврського) **рівня вищої освіти**
(першого (бакалаврського), другого (магістерського))

зі спеціальності7.050102, 8.050102 Інформаційні технології проектування
7.050103, 8.050103 Системне проектування
(код та назва спеціальності)

на тему: Система управління розумним домом. Підсистема забезпечення безпеки

Виконав (-ла): студент (-ка) _4___ курсу, групи __ДА12_____
(шифр групи)

Євтух Богдан Віталійович _____ _____
(прізвище, ім'я, по батькові) (підпис)

Керівник ст.. викладач Бритов О.А _____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант Охорона праці доцент, кандидат наук, Гусєв А.М. _____
(назва розділу) (посада, вчене звання, науковий ступінь, прізвище, ініціали) (підпис)

Рецензент доцент каф. ММСА ІПСА, к.т.н., доц,Тимошенко Ю. А. _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Нормоконтроль ст.. викладач Бритов О.А. _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2015 року

Національний технічний університет України
«Київський політехнічний інститут»

Факультет (інститут) ННК "Інститут прикладного системного аналізу"
(повна назва)

Кафедра Системного проектування
(повна назва)

Рівень вищої освіти Перший(Бакалаврський)
(перший (бакалаврський), другий (магістерський) або спеціаліста)

Спеціальність
7.050103, 8.050103 Системне проектування
(код і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ А.І.Петренко
(підпис) (ініціали, прізвище)
«___»_____2015 р.

ЗАВДАННЯ
на дипломний проект (роботу) студенту
Євтуху Богдану Віталійовичу
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи)) Система управління розумним домом. Підсистема забезпечення безпеки.
керівник проекту (роботи))Британов Олексій Анатолійович, ст. викладач ,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «___»_____ 2015 р. №_____

2. Строк подання студентом проекту (роботи) 19.06.2015

3. Вихідні дані до проекту (роботи) _____

Операційна система Android
Зона «довіри» сервер
Форма реалізації: теоретична схема для управління, схема потоку даних, бібліотека для забезпечення безпеки.
В якості реалізації алгоритмів можна використовувати стандартні Android рішення

4. Зміст розрахунково-пояснювальної записки (перелік завдань, які потрібно розробити)

1. Розглянути можливі алгоритми шифрування даних, стандартні схеми захисту.

2. Розробити алгоритм шифрування. Обрати схему захисту.
3. Розробити тести для перевірки роботи системи шифрування.
5. Розробити програмну реалізацію безпечної передачі даних.
6. Розглянути можливі варіанти систем управління розумним домом.
7. Обрати або створити систему управління розумним домом.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслеників, плакатів тощо)

1. Діаграма класів – плакат.
2. Діаграма послідовностей – плакат.
3. Діаграма прецедентів – плакат.
4. Діаграма Aris – плакат.

6. Консультанти розділів проекту (роботи)*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Гусєв А.М., доцент		

7. Дата видачі завдання 01.02.2015

* Консультантом не може бути зазначено керівника дипломного проекту (роботи).

Календарний план

№ з/п	Назва етапів виконання дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Отримання завдання	01.02.2015	
2	Збір інформації	15.02.2015	
3	Вивчення варіантів реалізації та вибір варіанту для розробки	28.02.2015	
4	Розглянути можливі алгоритми шифрування даних, стандартні схеми захисту.	10.03.2015	
5	Розробити алгоритм шифрування. Обрати схему захисту.	15.03.2015	
6	Розробити тести для перевірки роботи системи шифрування та управління.	25.03.2015	
7	Розробити програмну реалізацію безпечної передачі даних.	25.04.2015	
8	Тестування отриманого модуля.	30.04.2015	
9	Оформлення дипломної роботи	31.05.2015	
10	Отримання допуску до захисту та подача роботи в ДЕК	19.06.2015	

Студент _____ Б.В. Євтух
(підпис) (ініціали, прізвище)

Керівник проекту (роботи) _____ О.А. Бритов
(підпис) (ініціали, прізвище)

АНОТАЦІЯ

до бакалаврської дипломної роботі Євтуха Богдана Віталійовича
на тему: «Система управління розумним будинком. Підсистема забезпечення безпеки »

Дипломна робота присвячена розробці системи управління розумним будинком, що включає в себе контроль над усіма параметрами, а саме: освітлення, температура, вологість; і підсистеми для безпечної передачі даних на основі PKI. У роботі також було проаналізовано основні криптографічні схеми, їх рівень надійності. Велика увага приділяється на алгоритми шифрування, такі як: RSA, AES, DES (Triple DES), еліптичні криві, Base64; і схеми захисту: симетричні, з відкритим ключем, PKI. Проведена порівняльна характеристика вищевказаних алгоритмів, визначено їх недоліки та сфери застосування. Розроблений модуль безпечної передачі даних може бути використаний в будь-якому клієнт-серверному додатку, забезпечуючи таким чином високу надійність.

Загальний обсяг роботи 74 сторінки, 14 рисунків, 5 таблиць, 19 бібліографічних найменувань.

Ключові слова: PKI, AES, DES, Triple DES, RSA, еліптичні криві, розумний будинок, клієнт-серверний додаток, управління.

АННОТАЦИЯ

к бакалаврской дипломной работе Евтуха Богдана Витальевича
на тему:«Система управления умным домом. Подсистема обеспечения безопасности»

Дипломная работа посвящена разработке системы управления умным домом, что включает в себя контроль над всеми параметрами, а именно: освещение, температура, влажность; и подсистемы для безопасной передачи данных на основе PKI. В работе также были проанализированы основные криптографические схемы, их уровень надежности. Большое внимание уделяется на алгоритмы шифрования, такие как: RSA, AES, DES (Triple DES), эллиптические кривые, Base64; и схемы защиты: симметричные, с открытым ключом, PKI. Проведена сравнительная характеристика вышеуказанных алгоритмов, определены их недостатки и сферы применения. Разработанный модуль безопасной передачи данных может быть использован в любом клиент-серверном приложении, обеспечивая таким образом высокую надежность.

Общий объем работы 74 страницы, 14 рисунков, 5 таблиц, 19 библиографических наименований.

Ключевые слова: PKI, AES, DES, Triple DES, RSA, эллиптические кривые, умный дом, клиент-серверное приложение, управление.

AN ABSTRACT OF THE THESIS OF

Bohdan Yevtukh for the degree bachelor of the computer science in NTUU “KPI”

Title: “Smart home control system. Security subsystem.”

Thesis is dedicated to the development of smart home control system that includes the control of all parameters, such as: lighting, temperature, humidity; and subsystems for the secure transmission of data based on PKI. The paper also analyzed the main cryptographic schemes and their reliability. Much attention is given to the encryption algorithms, such as: RSA, AES, DES (Triple DES), elliptic curves, Base64; and protection schemes: symmetrical, public key scheme, PKI. The comparative characteristic of the above algorithms, identified their shortcomings and scope. Designed secure data transmission module can be used in any client-server applications, thus ensuring high reliability.

The total amount of work 74 pages, 14 figures, 5 tables, 19 bibliographic references.

Keywords: PKI, AES, DES, Triple DES, RSA, elliptic curves, smart home, client-server application.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

Розумний дім – будинок з мікроконтроллерами, що керують всіма або більшою частиною пристроїв всередині.

GPS (Global Positioning System) – система для отримання місцезнаходження об’єкта.

Атака – загальна назва спроби заподіяти шкоду інформаційному носію.

Автоматизований – пристрій, який працює

Шифротекст – видозмінений текст (набір символів, що не несуть інформації за умови відсутності ключа).

Вразливість інформації – властивість інформації, за якої зловмисник хоче змінити, знищити чи отримати її.

AES (Advanced Encryption Standard) – симетричний шифр (стандарт).

DES (Data Encryption Standard) – симетричний шифр.

RSA (Rivest, Shamir, Adleman) – асиметричний шифр.

PKI (Public Key Infrastructure) – інфраструктура відкритих ключів.

Криптографічна стійкість – рівень захищеності.

Зона «довіри» – канал, який не можуть прослуховувати злочинці.

GSM (Group Special Mobile) – глобальна система мобільного зв’язку.

SDL (Software Development Life Circle) – методика створення програмних продуктів.

ВСТУП

Будь-який будинок - будь-то адміністративний, виробничий або житловий складається з деякого набору підсистем, що відповідають за виконання певних функцій, які вирішують різні завдання в процесі функціонування цієї будівлі. У міру ускладнення цих підсистем і збільшення кількості, виконуваних ними функцій, управління ними ставало все складніше. Також стрімко зростають витрати на утримання обслуговуючого персоналу, ремонт та обслуговування цих підсистем. Вперше ці проблеми постали при експлуатації великих адміністративних і виробничих комплексів.

Сучасна будівля такого типу - це місто в мініатюрі. Фактично в ньому діють всі служби, що були раніше неодмінними атрибутами міського господарства. У таких будівлях зазвичай існує адміністративна служба або адміністратор, які використовують і обслуговують цю систему практично цілодобово. Хоча є чимало засобів автоматики, які самі справляються з покладеними на них завданнями, такими, як опалення, вентиляція, підтримка мікроклімату, освітлення, пожежна сигналізація, контроль входу / виходу і т.д., але управління і обслуговування всіх цих систем вимагає наявність адмініструє персоналу.

Його обов'язком є контроль роботи цих підсистем та вжиття заходів у разі виходу їх з ладу. Але є ситуації, коли навіть дії кваліфікованого персоналу можуть виявитися неефективними. Це випадки виникнення загрози будівлі і знаходилися в ньому людям, що мають глобальний характер - пожежа, землетрус та інші стихійні лиха, терористичні атаки. Тут потрібно приймати екстраординарні заходи в лічені частки секунди. Реакція і коректність дій людей в критичній ситуації може виявитися недостатньою.

Традиційні системи забезпечення різних аспектів життєдіяльності в минулому проектувалися як автономні. Такі системи, що створювалися окремо для кожної функції і об'єднані для довільної частини будівлі. У будинках встановлювалися системи тільки з тими можливостями і з тим ступенем

складності, які були необхідні на поточний момент побудови будівлі. Подальше розширення і модернізація даних систем були складними і дорогими завданнями через безліч різних чинників. Витрати на експлуатацію такої системи складаються з витрат на експлуатацію кожної автономної системи окремо, вартості навчання персоналу Вартість експлуатації цих систем висока - в силу їх автономності кожна з них підтримується окремо. Вартість навчання персоналу настільки ж висока, оскільки оператори повинні бути ознайомлені з експлуатацією кожної автономної системи.

Також не останнє місце займає питання безпечності інформації, адже маючи доступ до такого будинку можна завдати дуже великої шкоди його власнику. Оскільки в наш час досить поширеним являється віддалене керування, доступ до інформації, тощо, слід використовувати захищені схеми, схеми шифрування та захисту, щоб мінімізувати вразливості та не дати можливість злочинцю завдати шкоди.

РОЗУМНИЙ ДІМ. ІСТОРІЯ РОЗВИТКУ. КОНЦЕПЦІЇ. АВТОМАТИЗАЦІЯ.

1.1 Історія розвитку.

Перші «розумні будинки» з'явилися природно в США, ще в 50-ті роки минулого сторіччя. На той момент це були дійсно унікальні квартир, обладнані спеціальною електронікою, яка злагодити за багатьма речами в будинку, наприклад за пральними машинами, телевізорами, мікрохвильовими печами і т.д. Всі ці побутові прилади були об'єднані в одне ціле, і управляли з одного пульта, при цьому була можливість контролювати відключення, включення і деякі інші особливості роботи. З часом в країні стали з'являтися інтелектуальні будівлі, які вже були повністю обладнані різної автоматикою, об'єднаної в єдину мережу. У цей час розвиток стало бурхливим, дослідники та розробники стали приділяти особливу увагу не тільки комфортабельності, але і безпеки, а також економії ресурсів завдяки системі «розумний дім».

Кошти, які вкладалися в розробку нових технологій для інтелектуальних будівель, були величезними, люди вірили, що в майбутньому це принесе непоганий прибуток. Починаючи з 1978 року, розробники змогли добитися управління електричними побутовими приладами через звичайні дроти, де проходило електрику напругою в 110В.[11] Це був справжній прорив, який дозволив надалі здійснювати розвиток за даною схемою. Особливий розвиток почалося в 90-і роки, коли з'явилася чимала кількість різних датчиків і сенсорів, без яких навіть неможливо уявити процес автоматизації.

Сучасний «розумний дім» втілив у собі безліч інноваційних розробок, які зробили його унікальним з безпеки і комфортабельності. Наявність всіх цих розробок дозволяє сьогодні втілювати мрії в життя, тепер власнику житла зовсім необов'язково турбуватися про свій будинок, адже він завжди під контролем обладнання, яке не дає збоїв і працює цілодобово весь рік, навіть коли нікого немає в будинку. Зараз на ринку є чимало компаній, що пропонують свої послуги

у сфері проектування «розумних будинків», при виборі тієї або іншої компанії, необхідно бути впевненим у професіоналізмі співробітників, щоб надалі не випробовувати проблем з технікою.

1.2. Концепції розумного дому.

У кожному сучасному будинку (будинку) в тій чи й іншій мірі функціонує велика кількість обладнання, що забезпечує побут, комфорт, затишок, зв'язок і безпеку, що допомагає відпочити і створює повноцінне робоче середовище. Зручність управління цими системами, їх інтеграція один з одним, можливість злагоджено працювати разом, збільшуючи тим самим функціональність кожної з них окремо - все це і дає можливість назвати такий будинок - Розумним домом.

У відсутності людини Розумний будинок буде підтримувати оптимальним чином постійний мікроклімат, зберігаючи тим самим затишок, кімнатні рослини і меблі. Вона вимкне не потрібен світло або навпаки буде створювати видимість вашої присутності, включаючи і вимикаючи освітлення в тій або іншій кімнаті час від часу. Розумний будинок дозволить Вам спокійно і безтурботно відпочивати.

Розумний будинок буде постійно стежити за всіма інженерними системами в будинку і не допустить спалаху або вибуху пов'язаного з витоком газу або зіпсованої меблів через витік води.

Також не залишиться непоміченим проникнення в будинок стороннього. Система Розумний будинок постарається випровадити його сам, створюючи неприємні умови його знаходження в будинку і, звичайно, він повідомить Вам і на пульт охорони про цю подію, скориставшись мобільним зв'язком або електронною поштою.[14]

Господар може повідомляти Розумному будинку не тільки про те, що він повертається, але постійно може керувати їй і отримувати інформацію про стан

систем в будинку, перебуваючи при цьому, де завгодно. Тому вам не потрібна більше нянька, яка буде стежити, щоб діти не сиділи перед телевізором, поки В

ас немає вдома. Ви зможете зробити це самі - віддалено. І Ваш Розумний будинок допоможе Вам у цьому.

1.3. Система інтелектуальної автоматизації.

Розумний будинок - це система інтелектуальної автоматики для управління інженерними системами сучасної будівлі.

Будь-якій людині в будинку, в квартирі або в офісі важливо відчувати себе комфортно і в безпеці. Саме ці два завдання плюс естетика зовнішнього вигляду пристроїв - і є основні цільові установки, на які орієнтовані системи «Розумний Дім». Інтелектуальна автоматика управляє всіма інженерними системами в будинку, дозволяє людині централізовано встановлювати комфортні для себе - температуру, вологість, освітленість в кімнатах, зонах, і забезпечує безпеку.

Система Розумний Дім включає в себе наступні об'єкти автоматизації:

- Управління освітленням;
- Управління електроприводами;
- Клімат контроль;
- Управління системою вентиляції;
- Централізоване управління системами:
- Домашнього кінотеатру;
- Мультірум;
- Системи відеоспостереження;
- ОПС (охоронно-пожежна сигналізація);
- СКД (системи контролю доступу);
- Контроль навантажень і аварійних станів;
- Управління інженерним обладнанням з сенсорних панелей;

- Сервер управління.

Система Розумний Дім забезпечує механізм централізованого контролю та інтелектуального управління в житлових, офісних або громадських приміщеннях.[15] З інсталяцією подібної системи вдома чи на роботі кожен користувач отримує можливість:

В рамках загальної середовища проживання задавати параметри власної індивідуальної середовища (світло, температура повітря, звук і т.д.), в т.ч. порядок роботи системи:

- Здійснювати управління необхідною системою (освітлення, клімат, відеоспостереження тощо)
- Отримувати доступ до інформації про стан всіх систем життєзабезпечення будинку (перебуваючи всередині нього або віддалено)
- Загальна схема системи управління виглядає наступним чином:
- Центральний процесор управління / головний блок управління
- Датчики (температури, освітленості, задимленості, руху та ін.)
- Керуючі пристрої (диммери, реле, ІЧ-емітери та ін.)
- Інтерфейси управління (кнопкові вимикачі, пульти ІК і радіопульт, сенсорні панелі, web / wap інтерфейс)
- Власна мережа управління, що об'єднує вищевказані елементи
- Керовані пристрої (світильники, кондиціонери, компоненти домашнього кінотеатру та ін.)
- Допоміжні мережі (Ethernet, телефонна мережа, дистрибуція аудіо і відеосигналу)
- Програмне забезпечення проекту

Основна функція центрального процесора - управління підпорядкованими йому пристроями з використанням наступних інтерфейсів: Ethernet, RS-232, RS-485, IR, аналогових і цифрових входів / виходів та ін. Також центральний

процесор управління містить багатозадачну операційну систему, інструментальні засоби програмування і в деяких випадках Web сервер. Датчики розташовуються в певних місцях квартири, які безпосередньо або через проміжні пристрої зв'язані єдиною мережею. Інтерфейси управління здійснюють загальне управління системами Розумний будинок.[12]

Загальний алгоритм роботи системи Розумний Дім

- По власної мережі управління інформація від датчиків або інтерфейсів надходить до центрального процесора управління.
- Програмне забезпечення центрального процесора обробляє отриману інформацію і генерує команди для керуючих пристроїв.

Команди надходять як з власної мережі, так і по допоміжної. Способи генерації команд, а також форма і склад відображуваної інформації про стан систем закладається на етапі розробки програмного забезпечення з урахуванням вимог проекту.

1.4. Висновки

Проведено огляд та аналіз систем розумного дому. Вони почали набирати темпи розвитку нещодавно, але основні положення були сформульовані досить давно, оскільки за відсутністю необхідного програмного та апаратного забезпечення неможливо створити системи подібного рівня.

Отже, розумний дім складається з таких частин:

- Пристрої – безпосередньо всі електронні побудові речі, контроль над якими необхідно автоматизувати.
- Датчики – пристрої керування та збору інформації розумного дому. Саме вони виконують роль одиниці в подібних системах.

- Мікроконтролери – апаратні системи, що об’єднують датчики в групи, розрізняють також центральний процесор управління – мікроконтролер, що посилає від сервера інформацію в кінцеві вузли.
- Сервер – комп’ютер, який створює інтерфейс між користувачем та системою розумного дому. Саме він відповідає за надійність, функціональність.
- Канали передачі даних – логічні та фізичні канали, по яким передаються дані з урахуванням потреб (безпека, швидкість тощо).
- Хмара – зовнішня служба, що виконую роль бази даних для статистики та іншої службової інформації.
- Мобільні пристрої – пристрої, за допомогою яких користувач через сервер керує системою розумного дому.

СИСТЕМА УПРАВЛІННЯ РОЗУМНИМ ДОМОМ

2.1. Базова концепція

Система управління являє собою сукупність апаратних та програмних засобів, які насамперед націлені на економічність, тобто на зниження можливих розходів (електроенергія, тепло) користувача, а також надає додаткові можливості, наприклад, контроль присутності.[13] Розглянемо всі функції більш детально.

2.2. Енергозбереження

Енергозберігаюча система управління освітленням в багатоповерхових будинках (під'їзди, автостоянки, прибудинкові території, підвали, горища) дозволить знизити кількість споживаної електроенергії в 10-15 разів. У цих системах застосовується пристрій управління освітленням з роздільними силовими компонентами, що дозволяє використовувати існуючі лінії електропередач. Енергозберігаюче освітлення починається з намагання упорядкування часу роботи освітлювальних приладів. Ефективний захід енергозбереження - централізація управління освітленням з використанням спеціально розроблених графіків включення і виключення світла. Певну економію можна отримати за рахунок максимального використання всередині приміщення природного світла. Це досягається за рахунок правильного планування будівлі і використовуваних приміщень. Великий ефект дає використання енергозберігаючих ламп. Однак навіть сама «економна» лампа, якщо вона горить в порожньому приміщенні, стане безглуздим джерелом енерговитрат.

Найкраще енергозбереження забезпечують автоматичні вимикачі світла з використанням інфрачервоних та електронних датчиків. Електронні датчики вимірюють рівень освітленості приміщення і, при досягненні заданого

значення, видають команду на включення або виключення освітлення (датчики освітленості), або безпосередньо «бачать», що до приміщення увійшов чоловік, і вмикають світло (датчики руху). Світлочутливий елемент блокує ввімкнення освітлення при достатньому природному освітленні. Оскільки на відміну від реле-датчиків часу датчики руху вмикають світло тільки на час фактичного присутності людини в приміщенні, а витрати електроенергії на освітлення можуть бути знижені в кілька разів.

Для сходових кліток, коридорів і ліфтових холів економія додатково збільшується за рахунок поетажного управління освітлювальними приладами. В енергозберігаючих вимикачах освітлення застосовуються також інфрачервоні датчики руху з урахуванням планування приміщення.[16] Інші електронні датчики (датчики присутності) здатні визначити знаходження людей в приміщенні і тільки в цьому випадку тримають світло включеним. Інфрачервоний датчик «бачить» тільки рухається людини, хоча цей рух може бути і невеликим - наприклад, помах рукою або кивок головою. При великих часах затримки інфрачервоний датчик працює в режимі датчика присутності, тобто підтримує освітлення при тривалому присутності в приміщенні людей. Малий час затримки вибирається при використанні інфрачервоних датчиків як датчика руху в прохідних приміщеннях. Електронні вимикачі світла можуть використовуватися як автономно, так і в складі автоматизованої системи управління, яку нині називають «розумний дім».

В основі системи енергозбереження лежить температурний контролер і електроконвектори російського і зарубіжного виробництва, що мають сучасний дизайн та доступні ціни. Вони не спалюють кисень, не сушать повітря, пожежобезпечні. Також, замість конвекторів можна використовувати гріють шнури (тепла підлога), інфрачервоні плівки і панелі, електрокотли універсальні і можуть працювати з будь-якими нагрівальними приладами. У традиційних водяних системах опалення датчики можуть управляти кранами з електроприводом або електроклапанами, встановленими на трубах опалення.

У розподільному щиті монтуються автоматичні вимикачі для захисту всіх елементів системи від перевантажень і струмів короткого замикання, а також силові виконавчі пристрої (СИУ-4, СИУ-1). У системах використовується тільки якісне та надійне електровстановлювальне обладнання провідних європейських фірм, найкращим чином зарекомендувало себе при монтажі та експлуатації. Управляється система температурним контролером за допомогою температурних датчиків і керованих розеток. Монтаж системи управління проводиться телефонним кабелем довжиною до 100 метрів.

2.3. Освітлення

В інтелектуальній системі «Розумний Дім» Ви можете керувати світлом натисненням однієї клавіші. За допомогою одного пульта ви зможете налаштувати лампи, люстри, світильники так, як вам подобається. Якщо Ви вирішили запросити гостей і створити їм затишну світлову атмосферу, то система «Розумний Дім» прийде вам на допомогу, Ви можете одним рухом руки міняти світлову гаму в приміщенні. Датчики руху забезпечують автоматичне перемикання світла, коли ви до них наближаєтеся.[11] Для забезпечення комфорту і затишку у Вашому будинку кожна кімната, хол, зал повинні бути добре освітлені. Без інтелектуальної системи «Розумний Дім» для цього буде потрібно установка великої кількості різних світлових приладів із заплутаною мережею вимикачів.

Система позбавить Вас від необхідності встановлювати безліч вимикачів, Вам представиться можливість замінити їх компактними сенсорними. Так з одного стандартного шести сенсорного вимикача можна управляти дванадцятьма світловими групами. Ви зможете, як плавно регулювати їх яскравість, так просто включити їх або вимкнути. За допомогою сенсорних вимикачів або панелей Ви легко зможете створювати різні світлові сцени, що, безсумнівно, додасть затишку і комфорту Вашого дому, наприклад, сцену «Вечір», при якій одна група світлових приладів включиться на певну

яскравість, інша група вимкнеться, штори закриються, а система клімат контролю перейде в комфортний режим. У нічний час світло в коридорах і прихожих буде включатися на частину яскравості автоматично при появі руху. Вам не доведеться шукати вимикач в темряві. Також системою освітлення можна управляти дистанційно з пульта, ноутбука або мобільного телефону. Ви під'їжджаєте до будинку вночі, а він зустріне Вас з включеним освітленням фасаду, підсвічуванням ландшафту і доріжок.

Управління освітленням - одна з найважливіших задач в будинку.[14] Завдяки інтелектуальному програмування можна заощадити електроенергію та термін експлуатації ламп. Відпадає необхідність шукати вимикачі світла в темряві, а так само вимикати світло при виході з кімнати. Інтелектуальна система вимкне світло, тільки після того як ви заснете і включить м'яке підсвічування, якщо ви прокинетеся вночі, щоб не дратувати очі яскравим світлом. А вранці система вирішить, яке освітлення потрібно в будинку залежно від погоди на вулиці.

Систему автоматизованого управління освітленням можна налаштувати таким чином, що вона буде визначати, в якій частині кімнати знаходиться людина і підсвічувати саме її. У заміському котеджі система може включати вечірню підсвітку двору і декоративне підсвічування фасаду будівлі. Вона зустрічає вас або ваш автомобіль у вечірній час включеним світлом у дворі і гаражі.

Але управління освітленням приносить не тільки комфорт. Розумний будинок може самостійно включати вечорами світло в квартирі, імітуючи присутність людей. Завдяки цьому, майно буде перебувати під подвійним захистом під час Вашої відпустки або тривалої відсутності.

2.4. Система клімат-контроль

Така система клімат-контролю працює на підставі закладених у неї алгоритмів, що дозволяють підтримувати встановлені параметри повітряного серед і різних кліматичних зон в приміщеннях при мінімальних затратах енергоресурсів.

Розглянута система дозволяє забезпечувати виконання різних операцій. З її допомогою проводиться нагрів або охолодження. При цьому виключається одночасна робота кондиціонера і системи опалення. Винятком тут може бути наявність теплої підлоги, підтримуючого встановлену температуру в нижній частині кондиціонером приміщення.

Така система забезпечує зниження температури в нічний час в безлюдних приміщеннях і спальнях, що дозволяє створити комфортні умови для сну, а також економити енергоресурси. Крім того, вона дає можливість мінімізувати роботу апаратури і обладнання під час відсутності господарів за допомогою використання режимів роботи «денне відсутність» і «відпустку». При включенні другого режиму проводиться повне відключення системи кондиціонування та вентиляції, а опалювальна система виводиться на мінімальний рівень потужності. Перед поверненням додому можна завчасно встановити в приміщеннях комфортний кліматичний режим шляхом активації системи клімат-контролю по телефону або через інтернет.[16]

Система управління кліматом в приміщенні дає можливість коригувати рівень температури, вологості, величину притоку свіжого повітря індивідуально для кожного приміщення, управляти роботою системи фільтрації повітря, створювати індивідуальну кліматичну систему для кожного члена сім'ї, погоду в будинку (наприклад, в кімнаті проживання дітей відсутність протягів при постійно свіжому повітрі). У теж час система клімат-контролю, незважаючи на виконання великої кількості функцій, забезпечує економію фінансових коштів і вирішує проблему енергозбереження. Наприклад, систему

можна налаштувати таким чином, що у вихідні дні та неробочий час подача тепла в приміщення скорочувалася або відключалася зовсім. Такий режим роботи особливо актуальний для використання в заміських котеджах із застосуванням в них автономних систем опалення. Зазначена система дозволяє дистанційно включати котел опалення або перемикати його в режим економії. З метою більш ефективної і раціональної організації життєдіяльності офісів можливо встановлення контролю над станом комунікацій теплопостачання, електропостачання, водопостачання, створення найбільш комфортних умов роботи для працівників компанії.

Система клімат-контролю «розумного будинку» виключить можливість псування колекції картин, книг або вин шляхом створення найбільш сприятливих умов для їх зберігання.

Для забезпечення коригування параметрів роботи системи застосовуються різні датчики, які фіксують поточні показники мікроклімату в приміщеннях будинку, а також засоби для управління у вигляді перемикачів і панелей. При їх використанні система здатна управляти якістю повітря (температурою, вологістю, озонуванням) відповідно до пори року і доби, режимом провітрювання з використанням автоматичної системи відкривання вікон, змінювати режим роботи радіаторів опалення та теплої підлоги, автоматично підтримувати температуру і вологість у спеціальних приміщеннях, а також аварійно зупиняти систему опалення.[12]

Таким чином, система клімат-контролю «розумного будинку» дозволяє створити здоровий і комфортний мікроклімат для затишного проживання в будинку

2.5. Контроль проникнення

Постановка і зняття квартири з охорони виробляються за допомогою кодової панелі, розміщеної у тамбурі. При відкритті вхідних дверей у людини є

30 секунд на введення правильного коду. Якщо ж код не буде введений розумний будинок включить сирени і відправить СМС повідомлення на кілька телефонних номерів.

Датчики руху, розташовані на кухні, спальні і вітальні дозволять виявити проникнення через вікна.

Рис 2.1 - Схема застосування датчиків руху в квартирі

інтелектуальна система розумний будинок

При виході з квартири достатньо ввести код на охоронній панелі і розумний будинок не тільки включить сигналізацію, але і відключить освітлення, переведе систему опалення в режим енергозбереження.

2.6. Контроль протікання води

Прорив труб водопостачання є дуже неприємною подією у зв'язку з псуванням не тільки свого, але і сусідського майна. Виявити і запобігти витоку

води так само допоможе розумний будинок. Контрольованими зонами є санвузли та кухня, тобто ті приміщення, де проходять труби водопостачання.

Прорив труби або перелив води через краї раковини фіксується за допомогою спеціальних датчиків. У випадку протікання розумний будинок перекроїть доступ води в квартиру і відправить СМС повідомлення на задані телефони.

Рис 2.2 – Схема використання датчиків протікання води

2.7. Висновки

Отже, в ході роботи над даним розділом було обрано систему управління над розумним домом, яка являє собою сукупність пидсистем керування окремими параметрами та групами датчиків/контролерів.

Було проаналізовано наступні групи контролю:

- Освітлення – відповідає за контроль над освітленістю дому, взаємодіє з групою знаходження.
- Енергозбереження – оптимізує роботу пристроїв.

- Клімат-контроль – регулює системи встановлення температури та вологості в залежності з потребами користувача.
- Проникнення – підсистема захисту від фізичного несанкціонованого вторгнення в дім.
- Знаходження – підсистема, що визначає, в якій кімнаті знаходиться користувач та окремо мобільні пристрої, визначені як керуючі елементи.
- Протікання води – система визначення та усунення проблем з протіканням води та, відповідно, оповіщуванням користувача.
- Штучного інтелекту – система, що на основі статистичних даних сама від імені користувача підлагоджує роботи всіх інших систем.

ПІДСИСТЕМА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ

3.1. Класифікація загроз безпеки інформації

3.1.1. Базові визначення

Під загрозою безпеки інформації розуміють подію або дію, яка може викликати зміну функціонування системи, пов'язане з порушенням захищеності оброблюваної в ній інформації.

Вразливість інформації - це можливість виникнення такого стану, при якому створюються умови для реалізації загроз безпеки інформації.

Атакою на інформаційну систему називають дії, що робляться порушником, яке полягає в пошуку і використанні тієї або іншої уразливості. Інакше кажучи, атака на КС є реалізацією загрози безпеки інформації в ній.

Проблеми, що виникають з безпекою передачі інформації при роботі в комп'ютерних мережах, можна розділити на три основні типи [17]:

• перехоплення інформації - цілісність інформації зберігається, але її конфіденційність порушена;

• модифікація інформації - вихідне повідомлення змінюється або повністю підміняється іншим і відсилається адресату;

• підміна авторства інформації. Дана проблема може мати серйозні наслідки. Наприклад, хтось може послати лист від чужого імені (цей вид обману прийнято називати Спуфінга) або Web - сервер може прикидатися електронним магазином, приймати замовлення, номери кредитних карт, але не висилати ніяких товарів.

Специфіка комп'ютерних мереж, з точки зору їх уразливості, пов'язана в основному з наявністю інтенсивного інформаційної взаємодії між територіально рознесеними і різнорідними (різнотипними) елементами.

Вразливими є буквально всі основні структурно-функціональні елементи КС: робочі станції, сервери (Host-машини), міжмережеві мости (шлюзи, центри комутації), канали зв'язку і т.д.

Відомо велика кількість різнопланових загроз безпеці інформації різного походження. У літературі зустрічається безліч різноманітних класифікацій, де в якості критеріїв розподілу використовуються види породжуваних небезпек, ступінь злого умислу, джерела появи загроз і т.д. Одна з найпростіших класифікацій наведена на рис. 3.1.

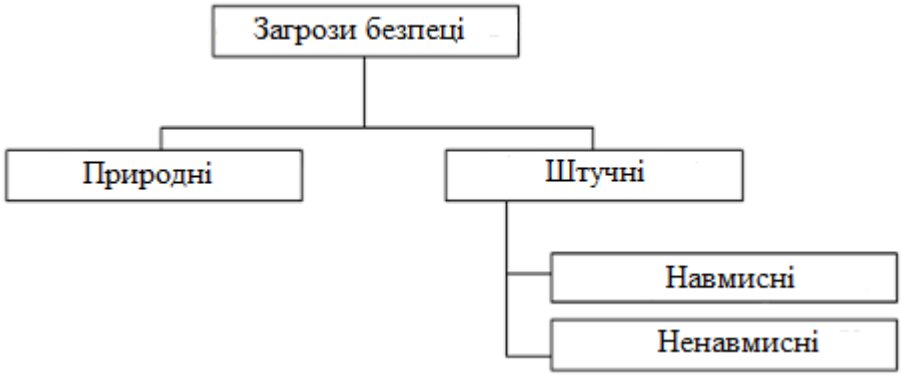

Рис. 3.1. Загальна класифікація загроз безпеки.

Природні загрози - це загрози, викликані впливами на інформаційну систему і її елементи об'єктивних фізичних процесів або стихійних природних явищ, незалежних від людини.

Штучні загрози - це загрози інформаційну систему, викликані діяльністю людини. Серед них, виходячи з мотивації дій, можна виділити:

- ненавмисні (ненавмисні, випадкові) загрози, викликані помилками в проектуванні інформаційну систему і її елементів, помилками в програмному забезпеченні, помилками в діях персоналу і т.п .;
- навмисні (навмисні) загрози, пов'язані з корисливими устремліннями людей (зловмисників).

Джерела загроз по відношенню до інформаційної системи можуть бути зовнішніми або внутрішніми (компоненти самої інформаційної системи - її апаратура, програми, персонал).[17]

Більш складна і детальна класифікація загроз наведена в Додатку А.

Аналіз негативних наслідків реалізації загроз припускає обов'язкову ідентифікацію можливих джерел загроз, вразливостей, що сприяють їх прояву і методів реалізації. І тоді ланцюжок виростає в схему, представлену на рис. 3.2.

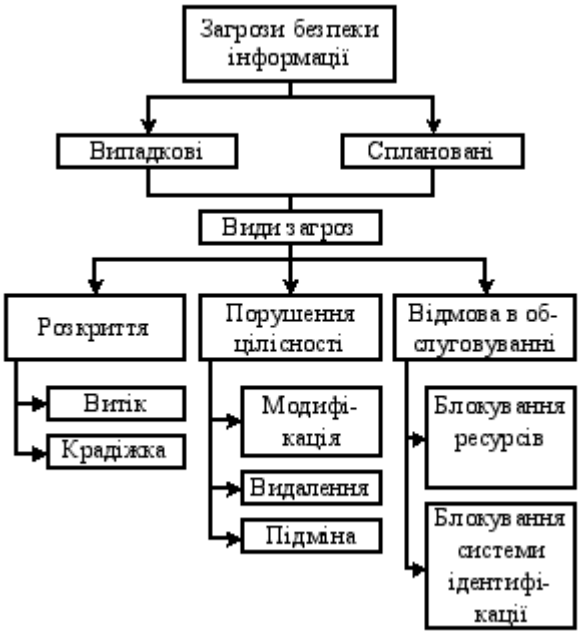

Рис. 3.2. Види загроз безпеки інформації в комп’ютерних мережах

Загрози класифікуються за можливості нанесення шкоди суб'єкту відносин при порушенні цілей безпеки [18]. Збиток може бути заподіяна будь-яким суб'єктом (злочин, вина або недбалість), а також стати наслідком, не залежних від суб'єкта проявів. Загроз не так вже й багато. При забезпеченні конфіденційності інформації це може бути розкрадання (копіювання) інформації і засобів її обробки, а також її втрата (ненавмисна втрата, витік). При забезпеченні цілісності інформації список загроз такий: модифікація (спотворення) інформації; заперечення автентичності інформації; нав'язування неправдивої інформації. При забезпеченні доступності інформації можливе її блокування, або знищення самої інформації і засобів її обробки.

Класифікація можливостей реалізації загроз (атак), являє собою сукупність можливих варіантів дій джерела загроз певними методами реалізації з використанням вразливостей, які призводять до реалізації цілей атаки. Мета атаки може не збігатися з метою реалізації загроз і може бути спрямована на отримання проміжного результату, необхідного для досягнення надалі реалізації загрози. У разі такого неспівпадіння атака розглядається як етап підготовки до вчинення дій, спрямованих на реалізацію загрози, тобто як «підготовка до вчинення» протиправної дії. Результатом атаки є наслідки, які є реалізацією загрози і / або сприяють такої реалізації.

Вихідними даними для проведення оцінки та аналізу загроз безпеки при роботі в мережі служать результати анкетування суб'єктів відносин, спрямовані на з'ясування спрямованості їх діяльності, передбачуваних пріоритетів цілей безпеки, завдань, що вирішуються в мережі і умов розташування та експлуатації мережі.

3.1.2. Найбільш поширені загрози

Найчастішими і найнебезпечнішими (з точки зору розміру шкоди) є ненавмисні помилки штатних користувачів, операторів, системних адміністраторів та інших осіб, які обслуговують комп'ютерну мережу [19].

Іноді такі помилки і є власне погрозами (неправильно введені дані або помилка в програмі, яка викликала крах системи), іноді вони створюють вразливі місця, якими можуть скористатися зловмисники (такі зазвичай помилки адміністрування). За деякими даними, до 65% втрат - наслідок ненавмисних помилок.

Пожежі та повені не приносять стільки бід, скільки безграмотність і недбалість у роботі.

Очевидно, найрадикальніший спосіб боротьби з ненавмисними помилками - максимальна автоматизація і строгий контроль.

Інші загрози доступності можна класифікувати за компонентами інформаційної системи, на які націлені загрози:

- відмова користувачів;
- внутрішній відмова мережі;
- відмова підтримуючої інфраструктури.

Зазвичай стосовно користувачам розглядаються наступні загрози:

- небажання працювати з інформаційною системою (найчастіше проявляється при необхідності освоювати нові можливості і при розбіжності між запитами користувачів і фактичними можливостями і технічними характеристиками);
- неможливість працювати з системою через відсутність відповідної підготовки (нестача загальної комп'ютерної грамотності, невміння інтерпретувати діагностичні повідомлення, невміння працювати з документацією тощо);
- неможливість працювати з системою в силу відсутності технічної підтримки (неповнота документації, недолік довідкової інформації тощо).

Основними джерелами внутрішніх відмов є:

- відступ (випадкове або навмисне) від встановлених правил експлуатації;
- вихід системи з штатного режиму експлуатації в силу випадкових або навмисних дій користувачів або обслуговуючого персоналу (перевищення розрахункового числа запитів, надмірний обсяг оброблюваної інформації тощо);
- помилки при (пере) конфигурировании системи;
- відмови програмного і апаратного забезпечення;
- руйнування даних;
- руйнування або пошкодження апаратури.

По відношенню до підтримуючої інфраструктурі рекомендується розглядати наступні загрози:

- Порушення роботи (випадкове або навмисне) систем зв'язку, електроживлення, водо- та / або теплопостачання, кондиціонування;
- руйнування або пошкодження приміщень;
- неможливість або небажання обслуговуючого персоналу та / або користувачів виконувати свої обов'язки (цивільні безлади, аварії на транспорті, терористичний акт або його загроза, страйк і т.п.).

Досить небезпечні так звані "скривджені" співробітники - нинішні і колишні. Як правило, вони прагнуть завдати шкоди організації - "кривднику", наприклад:

- зіпсувати обладнання;
- вбудувати логічну бомбу, яка з часом зруйнує програми та / або дані;
- видалити дані.

Скривджені співробітники, навіть колишні, знайомі з порядками в організації і здатні завдати чималої шкоди. Необхідно стежити за тим, щоб при

звільненні співробітника його права доступу (логічного і фізичного) до інформаційних ресурсів анулювалися.

3.1.3. Програмні атаки

Як засіб виведення мережі зі штатного режиму експлуатації може використовуватися агресивне споживання ресурсів (зазвичай - смуги пропускання мереж, обчислювальних можливостей процесорів або оперативної пам'яті). По розташуванню джерела загрози таке споживання підрозділяється на локальне та віддалене. При прорахунках в конфігурації системи локальна програма здатна практично монополізувати процесор і / або фізичну пам'ять, звівши швидкість виконання інших програм до нуля.

Найпростіший приклад віддаленого споживання ресурсів - атака, що отримала найменування "SYN-повінь" [17]. Вона являє собою спробу переповнити таблицю "напіввідкритих" TCP-з'єднань сервера (встановлення з'єднань починається, але не закінчується). Така атака щонайменше ускладнює встановлення нових сполук з боку легальних користувачів, тобто сервер виглядає як недоступний.

По відношенню до атаки "Papa Smurf" уразливі мережі, що сприймають ping-пакети з широкомовними адресами. Відповіді на такі пакети "з'їдають" смугу пропускання.

Віддалене споживання ресурсів останнім часом проявляється в особливо небезпечній формі - як скоординовані розподілені атаки, коли на сервер з безлічі різних адрес з максимальною швидкістю спрямовуються цілком легальні запити на з'єднання та / або обслуговування. Часом початку "моди" на подібні атаки можна вважати лютий 2000, коли жертвами виявилися кілька найбільших систем електронної комерції (точніше - власники та користувачі систем). Якщо має місце архітектурний прорахунок у вигляді розбалансованості між пропускною здатністю мережі і продуктивністю сервера, то захиститися від розподілених атак на доступність вкрай важко.

Для виведення систем зі штатного режиму експлуатації можуть використовуватися вразливі місця у вигляді програмних і апаратних помилок. Наприклад, відома помилка в процесорі Pentium I давала можливість локальному користувачеві шляхом виконання певної команди "підвісити" комп'ютер, так що допомагає тільки апаратний RESET [15].

Програма "Teardrop" віддалено "підвішує" комп'ютери, експлуатуючи помилку в збірці фрагментованих IP-пакетів [11].

3.1.4. Класифікація заходів забезпечення безпеки комп’ютерних систем

За способами здійснення всіх заходів забезпечення безпеки комп'ютерних мереж поділяються на: правові (законодавчі), морально-етичні, організаційні (адміністративні), фізичні, технічні (апаратно-програмні) [17,18].

До правових заходів захисту відносяться діючі в країні закони, укази та нормативні акти, що регламентують правила поводження з інформацією, що закріплюють права та обов'язки учасників інформаційних відносин у процесі її обробки та використання, а також встановлюють відповідальність за порушення цих правил, перешкоджаючи тим самим неправомірному використанню інформації і є стримуючим фактором для потенційних порушників.

До морально-етичним заходів протидії належать норми поведінки, які традиційно склалися або складаються в міру поширення комп'ютерних мереж у країні або суспільстві. Ці норми здебільшого не є обов'язковими, як законодавчо затверджені нормативні акти, проте, їх недотримання веде звичайно до падіння авторитету, престижу людини, групи осіб або організації. Морально-етичні норми бувають як неписані (наприклад, загальновизнані норми чесності, патріотизму і т.п.), так і писані, тобто оформлені в деякий звід (статут) правил чи приписів.

Організаційні (адміністративні) заходи захисту - це заходи організаційного характеру, що регламентують процеси функціонування системи обробки даних, використання її ресурсів, діяльність персоналу, а також порядок взаємодії користувачів із системою таким чином, щоб найбільшою мірою утруднити чи виключити можливість реалізації загроз безпеці. Вони включають [15]:

- заходи, здійснювані при проектуванні, будівництві та обладнанні мереж та інших об'єктів систем обробки даних;
- заходи щодо розробки правил доступу користувачів до ресурсів мереж (розробка політики безпеки);
- заходи, здійснювані при підборі й підготовці персоналу;
- організацію охорони і надійного пропускного режиму;
- організацію обліку, зберігання, використання та знищення документів і носіїв з інформацією;
- розподіл реквізитів розмежування доступу (паролів, ключів шифрування тощо);
- організацію явного і прихованого контролю за роботою користувачів;
- заходи, здійснювані при проектуванні, розробці, ремонті і модифікаціях обладнання та програмного забезпечення і т.п.

Фізичні заходи захисту засновані на застосуванні різного роду механічних, електро- або електронно-механічних пристроїв і споруд, спеціально призначених для створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних порушників до компонентів мереж і захищається, а також технічних засобів візуального спостереження, зв'язку та охоронної сигналізації.

Технічні (апаратні) заходи захисту засновані на використанні різних електронних пристроїв, що входять до складу КС і виконують (самостійно або в комплексі з іншими засобами) функції захисту.

Програмні методи захисту призначаються для безпосереднього захисту інформації за трьома напрямками: а) апаратури; б) програмного забезпечення; в) даних і керуючих команд.

Для захисту інформації при її передачі зазвичай використовують різні методи шифрування даних перед їх введенням в канал зв'язку або на фізичний носій з наступною розшифровкою. Як показує практика, методи шифрування дозволяють досить надійно приховати зміст повідомлення.

Всі програми захисту, що здійснюють управління доступом до машинної інформації, функціонують за принципом відповіді на питання: хто може виконувати, які операції і над якими даними.

Доступ може бути визначений як:

- загальний (безумовно що надається кожному користувачеві);
- відмова (безумовний відмову, наприклад дозвіл на видалення порції інформації);
- залежний від події (керований подією);
- залежний від змісту даних;
- залежний від стану (динамічного стану комп'ютерної системи);
- частотно-залежний (наприклад, доступ дозволений користувачеві тільки один чи певну кількість разів);
- по імені або іншим ознакою користувача;
- залежний від повноважень;
- за дозволом (наприклад, по паролю);
- за процедурою.

Також до ефективних заходів протидії спробам несанкціонованого доступу відносяться засоби реєстрації. Для цих цілей найбільш перспективними є нові операційні системи спеціального призначення, що широко застосовуються в зарубіжних країнах і отримали назву моніторингу (автоматичного спостереження за можливу комп'ютерної загрозою).

Моніторинг здійснюється самою операційною системою (ОС), причому в її обов'язки входить контроль за процесами введення-виведення, обробки та знищення машинної інформації. ОС фіксує час несанкціонованого доступу та програмних засобів, до яких був здійснений доступ. Крім цього, вона виробляє негайне оповіщення служби комп'ютерної безпеки про посягання на безпеку комп'ютерної системи з одночасною видачею на друк необхідних даних (лістингу). Останнім часом в США і низці європейських країн для захисту комп'ютерних систем діють також спеціальні підпрограми, що викликають самознищення основної програми при спробі несанкціонованого перегляду вмісту файлу з секретною інформацією за аналогією дії "логічної бомби".

Завдання забезпечення безпеки:

- Захист інформації в каналах зв'язку і базах даних криптографічними методами;
- Підтвердження автентичності об'єктів даних і користувачів (аутентифікація сторін, що встановлюють зв'язок);
- Виявлення порушень цілісності об'єктів даних;
- Забезпечення захисту технічних засобів і приміщень, в яких ведеться обробка конфіденційної інформації, від витоку по побічних каналах і від можливо впроваджених у них електронних пристроїв знімання інформації;
- Забезпечення захисту програмних продуктів і засобів обчислювальної техніки від впровадження в них програмних вірусів і закладок;

- Захист від несанкціонованих дій по каналу зв'язку від осіб, не допущених до засобам шифрування, але мають мети компрометації секретної інформації та дезорганізації роботи абонентських пунктів;
- Організаційно-технічні заходи, спрямовані на забезпечення схоронності конфіденційних даних.

3.2.Схема передачі даних розумного дому та виявлення потенційної небезпеки.

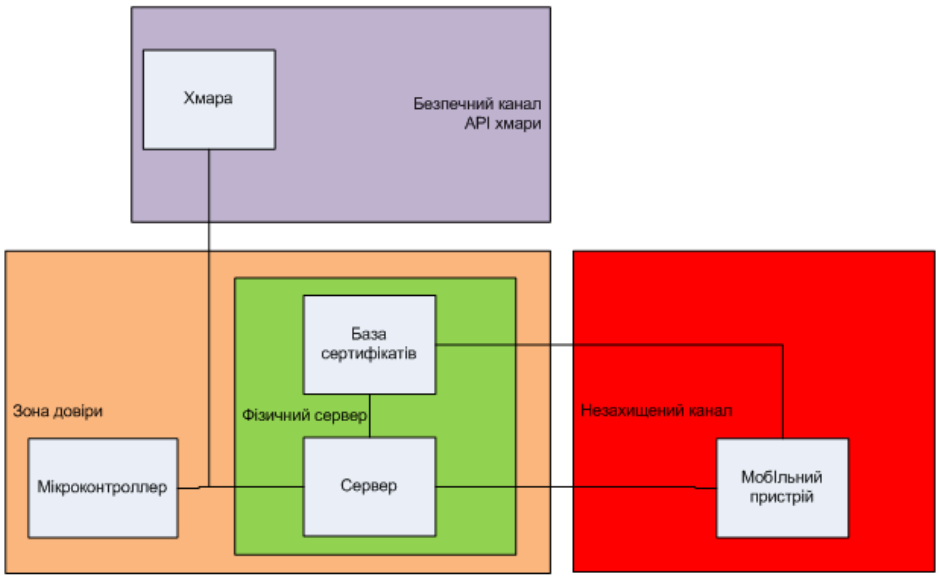

Рис. 3.1 Схема передачі даних

База сертифікатів – частина фізичного сервера, що зберігає всі цифрові підписи, до яких має повний доступ логічний сервер та частковий доступ користувач зі свого мобільного пристрою.

Мікроконтроллер – пристрій, що безпосередньо відповідає за керування розумним домом.

В рамках локальної мережі (мережі сервера) дані вважаються умовно захищеними.

Небезпеку становить незахищений канал користувача. Один з класичних сценаріїв – man-in-the-middle, тобто можливість інших осіб підключитись в канал між сервером та користувачем та видавати себе за когось з цих ключових осіб, беручи на себе роль невидимого посередника. Для того, щоб не допустити витік інформації, слід використовувати схеми з шифрування даних.

3.3. Схеми шифрування

3.3.1. Симетричні криптосистеми

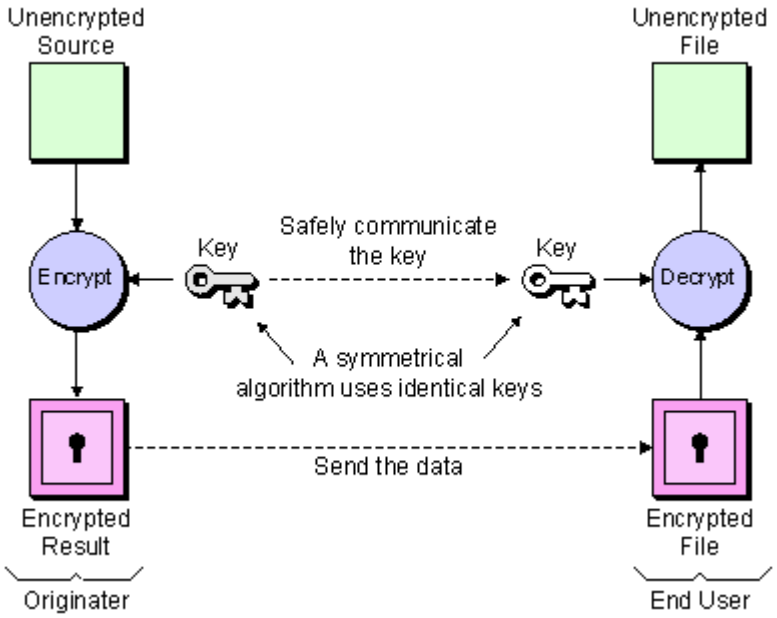

Рис. 3.2 Симетрична криптосистема

Симетричне шифрування передбачає використання одного і того ж ключа і для зашифрування, і для розшифрування. До симетричних алгоритмах застосовуються дві основні вимоги: повна втрата всіх статистичних закономірностей в об'єкті шифрування і відсутність лінійності. Прийнято розділяти симетричні системи на блокові і потокові. У блокових системах відбувається розбиття вихідних даних на блоки з подальшим перетворенням за допомогою ключа.

У поточних системах виробляється якась послідовність (вихідна гамма), яка в подальшому накладається на саме повідомлення, і шифрування даних відбувається потоком по мірі генерування гами. Схема зв'язку з використанням симетричною криптосистеми представлена на малюнку.

Схема зв'язку з використанням симетричною криптосистеми, де М - відкритий текст, К - секретний ключ, який передається по закритому каналу,

$E \cdot n$ (M) - операція зашифрування, а $D \cdot k$ (M) - операція розшифрування

Зазвичай при симетричному шифруванні використовується складна і багатоступенева комбінація підстановок і перестановок вихідних даних, причому ступенів (проходів) може бути безліч, при цьому кожній з них повинен відповідати «ключ проходу». Операція підстановки виконує перша вимога, що пред'являється до симетричного шифру, позбавляючись від будь-яких статистичних даних шляхом перемішування бітів повідомлення за певним заданим законом. Перестановка необхідна для виконання другої вимоги - додання алгоритмом нелінійності. Досягається це за рахунок заміни певної частини повідомлення заданого обсягу на стандартне значення шляхом звернення до вихідного масиву.

Симетричні системи мають як свої переваги, так і недоліки перед асиметричними. До переваг симетричних шифрів відносять високу швидкість шифрування, меншу необхідну довжину ключа при аналогічній стійкості, велику вивченість і простоту реалізації. Недоліками симетричних алгоритмів вважають в першу чергу складність обміну ключами зважаючи на велику ймовірність порушення секретності ключа при обміні, який необхідний, і складність управління ключами у великій мережі.

3.3.2. Системи з відкритим ключем

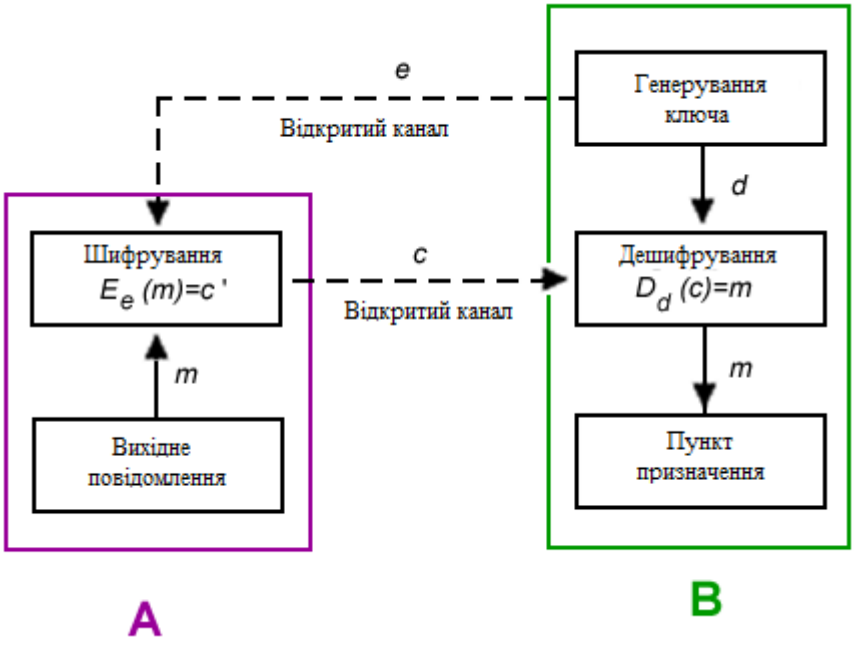

Рис. 3.3 Система з відкритим ключем

Відомо, що як би не були складні і надійні криптографічні системи - їх слабке місце при практичній реалізації - проблема розподілу ключів. Для того щоб був можливий обмін конфіденційною інформацією між двома суб'єктами ІС, ключ повинен бути згенерований одним з них, а потім якимось чином, знову ж у конфіденційному порядку, переданий іншому. Тобто в загальному випадку для передачі ключа знову ж потрібне використання якоїсь криптосистеми. Для вирішення цієї проблеми на основі результатів, отриманих класичної та сучасної алгеброю, були запропоновані системи з відкритим ключем.

Суть їх полягає в тому, що кожним адресатом ІС генеруються два ключі, зв'язані між собою за певним правилом. Один ключ оголошується відкритим, а інший закритим. Відкритий ключ публікується і доступний кожному, хто бажає послати повідомлення адресату. Секретний ключ зберігається в таємниці. Вихідний текст шифрується відкритим ключем адресата і передається йому. Зашифрований текст в принципі не може бути розшифрований тим же відкритим

ключем. Дешіфрованіе повідомлення можливо тільки з використанням закритого ключа, який відомий тільки самому адресату ...

У криптографії з відкритими ключами є ряд переваг перед класичною (тобто симетричною) криптографією. Найбільш корисне з них стосується управління ключами (зокрема, їх вибором і розсилкою). Давайте розглянемо стандартну симетричну криптосистему. Ключ шифрування є також ключем розшифрування, отже, перший не може бути розкритий. Це призводить до того, що дві легальні сторони (відправник і одержувач) домовляються заздалегідь про алгоритм зашифрування і ключах. Як вони це роблять? Або при особистій зустрічі, або при передачі по абсолютно секретному каналу. А що якщо такого каналу немає, і абоненти можуть перебувати в різних точках земної кулі?

При використанні ж криптосистем з відкритим ключем сторони не зобов'язані зустрічатися, знати один одного і мати суперсекретні канали зв'язку. Ця перевага стає ще більш актуальним у випадку великої кількості користувачів системи. Тоді, наприклад, один користувач може "закрито" зв'язатися з іншим, взявши деяку інформацію (відкритий ключ) із загальнодоступної бази даних (банку ключів).

Іншою важливою перевагою є довжина ключа. У симетричній криптографії, якщо ключ довше вихідного повідомлення, ніякого дійсного виграшу не досягається. Так як передбачається передавати ключ секретно, то чому б не передати саме повідомлення з цього секретному каналу? Звичайно, іноді обмін ключами відбувається заздалегідь - до передачі повідомлень. Що стосується криптосистем з відкритим ключем, то у них довжина ключа зашифрування не має значення, оскільки він відкритий і загальнодоступний. Тому і довжина ключа розшифрування не так важлива (одержувач тільки зберігає його в секретному місці). Зазначені вище дві переваги, що стосуються управління ключами, - головні для криптосистем з відкритим ключем. Але існують і інші плюси.

Різниця ключів (відкритого і особистого) в криптографії з відкритими ключами дозволило створити такі технології: електронні цифрові підписи, розподілена перевірка справжності, узгодження загального секретного ключа сесії, шифрування великих обсягів даних без попереднього обміну загальним секретним ключем.

Відомі алгоритми:

- RSA (Rivest-Shamir-Adleman)
- ECC (Elliptic Curve Cryptography)
- Алгоритм електронного цифрового підпису DSA (Digital Signature Algorithm, що входить до прийнятого в США державний стандарт цифрового підпису Digital Signature Standard, FIPS 1 86);
- Алгоритм DH (Diffie-Hellman), застосовуваний для вироблення спільного секретного ключа сесії.

3.3.3. Вразливість схем з відкритим ключем

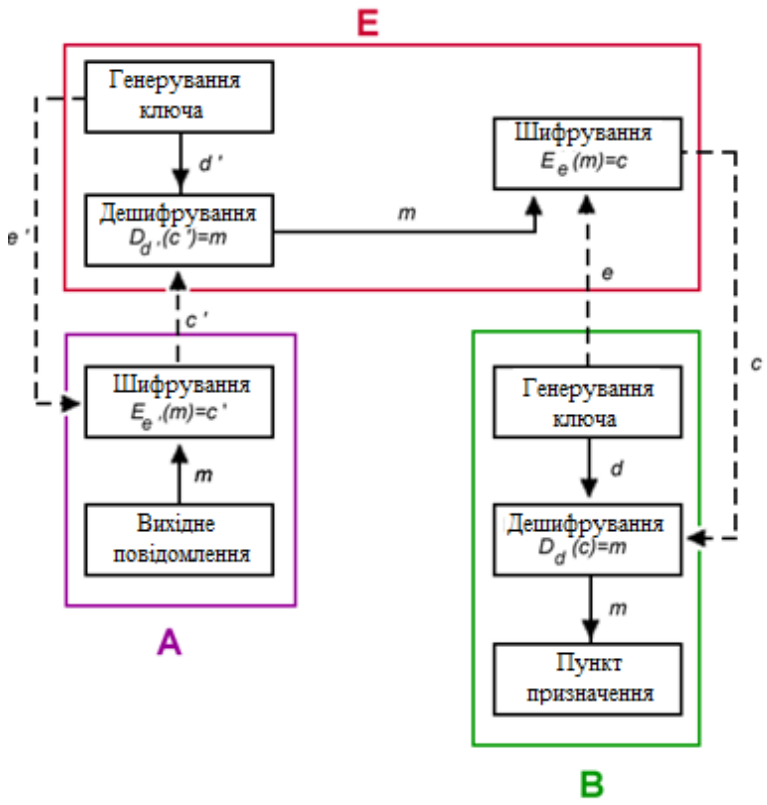

Рис 3.4 Вразливість схем з відкритим ключем

Здавалося б, що асиметричні алгоритми шифрування - ідеальна система, яка не потребує безпечного каналу для передачі ключа шифрування. Це передбачало б, що два легальних користувача могли б спілкуватися з відкритого каналу, не зустрічаючись, щоб обмінятися ключами. На жаль, це не так. Малюнок ілюструє, як Єва, що виконує роль активного перехоплювача, може захопити систему (розшифрувати повідомлення, призначене Бобу) без виламування системи шифрування[10].

Асиметричні алгоритми шифрування і активним перехватчіком.png

У цій моделі Єва перехоплює відкритий ключ e, посланий Бобом Алісі. Потім створює пару ключів e 'і d', «маскується» під Боба, посилаючи Алісі відкритий ключ e ', який, як думає Аліса, відкритий ключ, посланий їй Бобом. Єва перехоплює зашифровані повідомлення від Аліси до Боба, розшифровує їх за допомогою секретного ключа d ', заново зашифровує відкритим ключем e Боба і відправляє повідомлення Бобу. Таким чином, ніхто з учасників не здогадується, що є третя особа, яка може як просто перехопити повідомлення m, так і підмінити його на хибне повідомлення m '. Це підкреслює необхідність аутентифікації відкритих ключів. Для цього зазвичай використовують сертифікати. Розподілене управління ключами в PGP вирішує проблему за допомогою поручителів.

Ще одна форма атаки - обчислення закритого ключа, знаючи відкритий (малюнок нижче). Криптоаналітика знає алгоритм шифрування E, аналізуючи його, намагається знайти D. Цей процес спрощується, якщо криптоаналитик перехопив кілька криптотекстів c, посланих особою A особі B.[10]

Асиметрична криптосистема з пасивним перехватчіком.png

Більшість криптосистем з відкритим ключем засновані на проблемі факторизації великих чисел. Наприклад, RSA використовує в якості відкритого ключа n твір двох великих чисел. Складність злому такого алгоритму полягає в труднощі розкладання числа n на множники. Але це завдання вирішити реально. І з кожним роком процес розкладання стає все швидше

3.3.4. Інфраструктура відкритих ключів

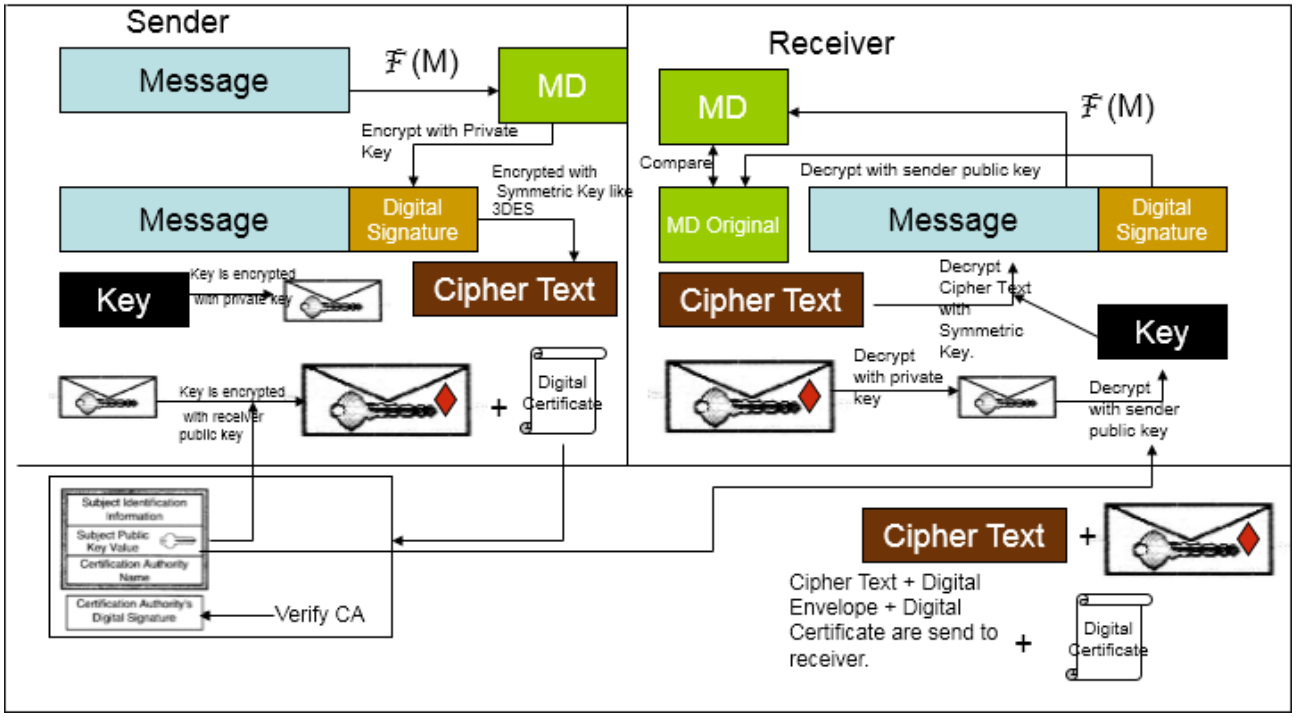

Рис. 3.5 PKI

Шифрування з відкритим ключем (також називається асиметричним ключем криптографія) використовує пару ключів для шифрування і дешифрування змісту. Пара ключів складається з одного громадськості та одного закритого ключа, математично пов'язані між собою. Людина, яка має намір спілкуватися надійно з іншими може поширювати відкритий ключ, але повинен тримати закритий ключ в таємниці. Вміст шифрується за допомогою однієї з клавіш можуть бути розшифровані за допомогою іншого. Припустимо, наприклад, що Боб хоче послати захищене повідомлення електронної пошти Алісі. Це може бути досягнуто таким чином:

І Аліса і Боб мають власні ключові пари. Вони зберегли свої ключі надійно себе і відправили їх відкриті ключі один з одним безпосередньо.

Боб використовує відкритий ключ Аліси зашифрувати повідомлення і відправляє його до неї.

Аліса використовує свій закритий ключ для розшифровки повідомлення.

Це спрощений приклад підкреслює принаймні одна очевидна занепокоєння Боб повинен мати про громадську ключем, який використовується для шифрування повідомлення. Тобто, він не може знати з упевненістю, що він ключ використовується для шифрування насправді належав до Аліси. Цілком можливо, що інша сторона моніторингу каналу зв'язку між Аліса і Боб заміщений інший ключ.

Концепція інфраструктури відкритого ключа перетворилася допомогти у вирішенні цієї проблеми та інші. Інфраструктура відкритих ключів (PKI) складається з програмного забезпечення та апаратних елементів, довірена третя сторона може використовувати, щоб встановити цілісність і право власності відкритого ключа. Довірена сторона, називається сертифікації (CA), як правило, це досягається шляхом видачі підписаних (шифрованих) довічних сертифікати, які підтверджують особистість суб'єкта сертифіката і пов'язують це ідентичність відкритого ключа, що міститься в сертифікаті. CA підписує сертифікат, використовуючи свій закритий ключ. Він видає відповідний відкритий ключ для всіх зацікавлених сторін у власний сертифікат ЦС. При використанні CA, попередній приклад може бути змінений таким чином:

Припустимо, що CA випустила цифровий сертифікат, який містить відкритий ключ. Са самостійно знаки цей сертифікат за допомогою закритого ключа, який відповідає відкритому ключу в сертифікаті.[10]

Аліса і Боб згодні використовувати CA для перевірки їх ідентичності.

Аліса просить сертифікат відкритого ключа з ЦС

CA перевіряє її особистість, обчислює хеш змісту, які будуть складати її сертифікат, підписує хеш за допомогою закритого ключа, відповідного відкритого ключа в опублікованому сертифікат ЦС, створює новий сертифікат, пов'язуючи зміст сертифікату та підписали хеш, і робить новий сертифікат публічно доступні.

Боб отримує сертифікат, розшифровує підписану плутанину з допомогою відкритого ключа центру сертифікації, обчислює новий хеш вмісту сертифіката

і порівнює два хешів. Якщо хеши збігаються, підпис перевіряється і Боб можуть вважати, що відкритий ключ в сертифікаті дійсно належить Алісі.
Боб використовує перевірити відкритий ключ Аліси для шифрування повідомлення з нею.

Аліса використовує свій закритий ключ для розшифровки повідомлення від Боба.

В цілому, процес підписання сертифіката дозволяє Боба, щоб перевірити, що відкритий ключ НЕ підроблений або пошкоджений під час транспортування. Перед видачею сертифікату, Каліфорнія хеши вміст, знаки (шифрує) хеш за допомогою власного секретного ключа, і включає в себе зашифрований хеш в виданого сертифіката. Боб перевіряє вміст сертифікату за допомогою розшифровки хеша з відкритим ключем CA, виконуючи окремий хеш вмісту сертифікатів, і порівнюючи два хешів. Якщо вони збігаються, Боб може бути достатньо впевнені, що сертифікат і відкритий ключ містить не були змінені.

Табл. 3.1 Структура PKI

Елемент	Опис
База сертифікатів	Зберігає всі дозволені сертифікати
Архів сертифікатів	Зберігає відмінені, заблоковані сертифікати.
Орган сертифікації	Корінь довіри PKI
Орган реєстрування	Система засвідчення.

3.4. Алгоритми шифрування

3.4.1. AES

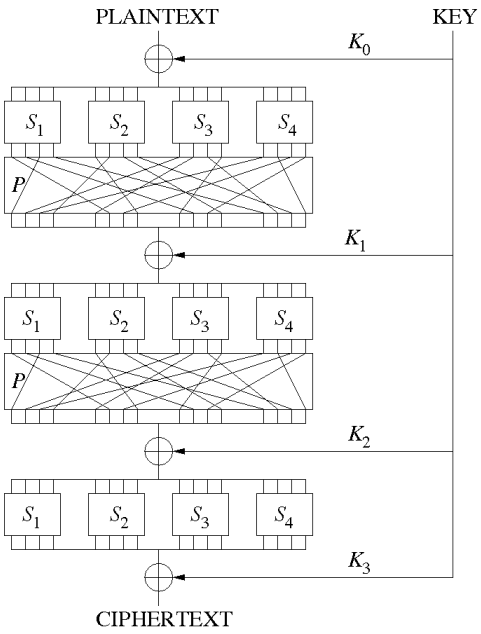

Рис. 3.6 SP

Є комбінацією S-box і P-box, які були розглянуті в документі des.docx, оскільки окремо вони не пропонують істотно кріптоустойчивость.[4]

S-box використовується для одиничної перестановки біт, після чого повідомлення передається на P-box, де воно «перемішується» (всі біти піддаються перестановки), потім складається по модулю з раундовим ключем і передається на наступний шар мережі.

Алгоритм:

- KeyExpansion - генерація раундових ключів.
- InitialRound
    - 2.1. AddRoundKey - додавання по модулю 2 проміжного масиву з раундовим ключем
- Rounds (для всіх раундів)
    - 3.1. SubBytes - нелінійна перестановка байт, використовуючи SP-мережі
    - 3.2. ShiftRows - циклічний зрушення 3 останніх рядків

- 3.3. MixColumns - комбінування (змішування) 4 байт кожного рядка з використанням обратнго лінійного перетворення
- 3.4. AddRoundKey

- FinalRound
  - 4.1. SubBytes
  - 4.2. ShiftRows
  - 4.3. AddRoundKey

Опишемо процедури більш докладно.

Використовуючи S-box (будується згідно властивостей поля Галуа $GF(2^8)$), відбувається незалежна заміна байт масиву State.

Береться зворотне число b в полі Галуа

$$\begin{Vmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{Vmatrix} = \begin{Vmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{Vmatrix} * \begin{Vmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{Vmatrix} + \begin{Vmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{Vmatrix}$$

Рис. 3.7 Операції перетворення

Таким чином, надається захист від атак, основаних на простих алгебраїчних властивостях.

Циклічний зсув кожного рядка вліво на певну величину, а саме на n-1, де n - номер рядка. Це справедливо у випадку використання блоків розміром 128 і 196 біт, для 256 біт ситуація дещо інша: зсув відбувається на n, для n! = 0.

Разом з попередньою процедурою вносить в шифротекст розсіювання. Крім змішування 4 байт кожного рядка, відбувається перемножування на фіксовану матрицю:

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

Рис. 3.8 Матриця перемноження

Трактується це таким чином:

Множення на 1 - ніяких змін.

Множення на 2 - зрушення вліво

Множення на 3 - зрушення вліво і підсумовування по модулю 2 з початковим значенням.

AES має досить просте математичне опис, але тим не менш є криптостійким і всі спроби знайти в ньому серйозну уразливість увінчалися невдачею. Єдиний спосіб боротьби зловмисників з AES - це атака не на саму захист, а на систему, використовуючи її уразливості.[7]

AES прийнятий як стандарт і широко використовується у всіх сферах (є одним з найпоширеніших). Intel процесора серії x86 включають в себе даний алгоритм шифрування.

3.4.2. RSA

Криптографічний асиметричний алгоритм (або алгоритм з відкритим ключем), побудований з використанням довгої арифметики і односторонніх функцій.

Односторонньої називається функція виду $y = f(x)$, яка володіє такими особливостями:

1. При відомому аргументі розрахувати функцію є тривіальним завданням, яка відносно просто може бути вирішена.

2. При відомому значенні функції знайти аргумент не представляється можливим з практичної точки зору. Іншими словами, за розумний час неможливо його знайти.

На відміну від симетричних шифрів, розрізняють public (відкритий) і private (закритий) ключі. У більшості випадків, відкритий ключ публікується, в той час як закритий тримається в строгому секреті. Це пов'язано з тим, що private ключ значно «більше» за розміром, ніж public, отже, його важче зламати.

Генерація ключів:

1. Вибір 2 простих цілих чисел (як правило, їх розмір як мінімум 1024 біт кожне) p і q.

2. Розрахунок модуля ключа як добуток: $n = p \cdot q$.

3. Розрахунок функції Ейлера: $F(n) = F(p) \cdot F(q) = (p-1) \cdot (q-1)$.

4. Вибір E - взаємно простого з $F(n)$. Як правило це просте число з невеликою кількістю одиничних біт. E називається відкритою експонентою і є частиною відкритого ключа. Важливо пам'ятати, що при виборі малих значеннях відкритої експоненти кріптоустойчивость може різко знизитися.[9]

5. Визначення закритою експоненти D, як мультиплікативно зворотного до E по модулю $F(n)$. Іншими словами, потрібно знайти таке D, щоб виконувалася така умова: $d \cdot e = 1 \; mod \; F(n)$. На практиці вона обчислюється за допомогою розширеного алгоритму Евкліда, який описаний нижче.

6. Пара $\{E, n\}$ - відритий ключ.

7. Пара $\{D, n\}$ - закритий ключ.

Алгоритм шифрування:

1. Переклад повідомлення M в число m. Не важко здогадатися, що цей пункт визначає сферу використання RSA як підпис, оскільки великі повідомлення не доцільно шифрувати таким способом. На практиці за допомогою RSA найчастіше шифрують симетричний ключ, наприклад AES, (для безпечної його передачі по каналу зв'язку) а останній використовують безпосередньо для шифрування даних.[10]

2. Взяти відкритий ключ $\{E, n\}$.

3. шіфротекста C визначається за формулою:

$$C = m \cdot E \; (mod \; n)$$

Алгоритм розшифрування:

1. Прийняти шифротекст C.

2. Взяти свій закритий ключ $\{D, n\}$.

3. Початкове повідомлення визначається за формулою:

$$m = C \cdot D \ (mod\ n)$$

Примітка: якщо сеансовий ключ більше, ніж n, тоді його розбивають на блоки потрібної довжини і шифрують окремо.

Розширений алгоритм Евкліда (рішення рівняння типу $a \cdot x + b \cdot y = 1$):

1. Покладемо початкову одиничну матрицю $E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

2. Обчислимо залишок від ділення $r = a\ mod\ b$

3. Якщо $r = 0$, другий стовпець матриці E - рішення задачі (вектор $\begin{matrix} x \\ y \end{matrix}$)

4. З рівняння $a = b \cdot q + r$ виведемо $q = \frac{a \cdot r}{b}$

5. Замінимо $E = E \cdot \begin{bmatrix} 0 & 1 \\ 1 & 1 - q \end{bmatrix}$. Переходимо до пункту 2.

Примітка: якщо як а покласти E, а в якості b - модуль, тоді x - закрита експонента.

В результаті обчислення можна отримати негативну закриту експонента. Щоб змінити знак, достатньо використовувати наступну формулу:

$$D = (D + n)\ mod\ n$$

Криптостійкість:

Основним «проломом» у криптостійкості RSA може бути погано обрана відкрита експонента та / або пара простих чисел p і q. Завдання визначити секретну експоненту вкрай складна і вимагає занадто великої обчислювальної потужності і чималого інтервалу часу. Враховуючи той факт, що RSA ключі періодично змінюються (приблизно раз на рік), прямий злом не є практично досяжним завданням.

Застосування:

Як вже було сказано вище, RSA найчастіше використовують для цифрового підпису або шифрування іншого, більш «простого» ключа (що є практично однієї і тієї ж завданням). Причиною цьому є великі обчислювальні витрати, які визначають розміри вхідних повідомлень.

3.5. Вибір системи шифрування

Отже, проаналізуємо системи та алгоритми описані вище. Із систем найоптимальнішою є система з використанням PKI, адже саме вона забезпечую надійний канал для передачі сесійного ключа між сервером та клієнтом. В якості сертифікату візьмемо деякий ключ, відомий тільки користувачеві та базі сертифікатів (складова серверу в нашому випадку), причому база сертифікатів зберігає ключ в парі з публічним ключем користувача. Тоді система передачі даних буде приймати наступний вигляд (для зручності розіб’ємо на 2 етапи: авторизація та безпосередньо зв’язок між 2 вузлами):

- Авторизація
    - Клієнт підписує кодову фразу «SH0» (яка означає запит авторизації) своїм таємним ключем.
    - Сервер отримує повідомлення та надсилає його до бази сертифікатів.
    - Якщо база сертифікатів знаходить вказаний підпис, відбувається авторизація, а саме: сервер отримує з бази публічний ключ клієнта та надсилає йому зашифрований цим ключем AES сесійний ключ, включивши також фразу «SH1»; інакше генерується виключення «SH4»
- Сесія «спілкування»
    - Отримавши сесійний ключ, тепер клієнт та сервер можуть передавати один одному дані за допомогою кодової фрази «SH2»
        - По закінченню, клієнт відсилає «SH3» з закодованою фразою «exit», що призводить до припинення сесії та знищення сесійного ключа відповідно.

Раз на рік система сертифікатів повинна перегенеровувати ключі, щоб звести вірогідність злому до мінімуму.

Слід не забувати, що також є безпосередньо мікроконтроллери, що відповідають за зчитування та керування пристроями. З самого початку ми визначили локальну мережу сервера як «зона довіри», але існує ймовірність, що злочинець можу перебувати біля серверу, але відносно нетривалий час, тобто такий час, за який неможливо підібрати ключ для такого тривіального алгоритму шифрування, як Base64. Цей алгоритм досить добре підходить для таких цілей через те, що він не перевантажує відносно малопотужні мікроконтроллери, даючи таким чином деякий захист інформації, і в той же час не створює зайві затримки.

3.6.Тести підсистеми безпеки

Для перевірки коректної роботи описаного вище модуля запропоновані наступні тести:

- Перевірка на розрізнення команд
    - Спробувати почати з відправки повідомлення (SH2), очікуваний результат – виключення SH4.
    - Відправити запит на авторизацію (SH0) при використанні коректного сертифікату. Очікуваний результат – SH1
    - Відправити запит на авторизацію (SH0) при використанні неіснуючого сертифікату. Очікуваний результат – SH4
    - Завершити сесію та спробувати відправити повідомлення (SH2), очікується реакція SH4.
- Перевірка на коректність шифрування невеликих об’ємів даних
    - Зашифрувати повідомлення локально «Hello, World!»
    - Зашифрувати попереднє повідомлення та передати через Internet
    - Зашифрувати та відправити по мережі зображення

- Перевірка на коректність шифрування великих об’ємів даних
    - Зашифрувати файл з однотипних символів. Перевірити згенерований файл на «простоту».
    - Зашифрувати та передати повідомлення вагою до 1 МБ.
- Перевірка роботи системи сертифікатів
    - Використати функціонуючий сертифікат, що пов’язаний з даним мобільним пристроєм, очікується позитивна реакція
    - Використати робочий сертифікат іншого пристрою, очікується виключення
    - Використати неіснуючий сертифікат. Очікується виключення
- Спроба man-in-the-middle атаки
    - Створити міні-програму на серверній стороні, яка буде посередником між логічним сервером та клієнтом.
    - Підмінити коди. Очікуваний результат – виключення SH4 для будь-яких випадків.

3.7. Висновки

Отже, в ході роботи над даним розділом було досліджено роботу схем шифрування:

- Симетричні системи
- Системи з відкритим ключем
- Інфраструктура відкритих ключів

Алгоритми шифрування:

- Симетричні:
    - Base64
    - AES
    - DES
- Асиметричні:
    - RSA

- Еліптичні криві

Було визначено змішану схему шифрування, що використовує Base64, AES, RSA, тести для її перевірки та описано програмну реалізацію, що задовольняє їх.

ОХОРОНА ПРАЦІ ТА БЕЗПЕКИ В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Загальні положення

4.1.1. Теоретичні відомості охорони праці

Умови праці на робочому місці, безпека технологічних процесів, машин, механізмів, устаткування та інших засобів виробництва, стан засобів колективного та індивідуального захисту, що використовуються працівником, а також санітарно-побутові умови повинні відповідати вимогам нормативних актів про охорону праці. В законі України « Про охорону праці» визначається, що охорона праці - це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження життя, здоров'я і працездатності людини у процесі трудової діяльності.

На всіх підприємствах, в установах, організаціях повинні створюватися безпечні і нешкідливі умови праці. Забезпечення цих умов покладається на власника або уповноважений ним орган (далі роботодавець). Умови праці на робочому місці, безпека технологічних процесів, машин, механізмів, устаткування та інших засобів виробництва, стан засобів колективного та індивідуального захисту, що використовуються працівником, а також санітарно-побутові умови повинні відповідати вимогам нормативних актів про охорону праці. Роботодавець повинен впроваджувати сучасні засоби техніки безпеки, які запобігають виробничому травматизмові, і забезпечувати санітарно-гігієнічні умови, що запобігають виникненню професійних захворювань працівників. Він не має права вимагати від працівника виконання роботи, поєднаної з явною небезпекою для життя, а також в умовах, що не відповідають законодавству про охорону праці. Працівник має право відмовитися від дорученої роботи, якщо

створилася виробнича ситуація, небезпечна для його життя чи здоров'я або людей, які його оточують, і навколишнього середовища.

4.1.2. Санітарно-гігієнічні вимоги

Керівництво роботою по забезпеченню санітарно-побутових умов праці покладено на керівників структурних підрозділів.

Площу приміщень, в яких розташовують персональні комп'ютери, визначають згідно з чинними нормативними документами з розрахунку на одне робоче місце, обладнане ПК:

- площа - не менше 6,0 кв.м,
- обсяг - не менше 20,0 куб.м, з урахуванням максимальної кількості осіб, які одночасно працюють у зміні.
- робочі місця повинні бути розташовані на відстані не менше ніж 1 м. від стіни з вікном,
- відстань між бічними поверхнями комп'ютерів має бути не меншою за 1,2 м;
- відстань між тильною поверхнею одного комп'ютера та екраном іншого не повинна бути меншою 2,5 м;
- прохід між рядами робочих місць має бути не меншим 1 м.

Заземлені конструкції, що знаходяться в приміщеннях (батареї опалення, водопровідні труби, кабелі із заземленим відкритим екраном тощо), мають бути надійно захищені діелектричними щитками або сітками від випадкового дотику. В цих приміщеннях повинні бути медичні аптечки першої допомоги та система автоматичної пожежної сигналізації з димовими пожежними сповіщувачами та переносними вуглекислотними вогнегасниками з розрахунку 2 шт. на кожні 20 кв.м площі приміщення. Підходи до засобів пожежогасіння повинні бути вільними.

4.1.3. Вимоги до організації робочого місця

Конструкція робочого місця користувача ПК має забезпечувати підтримання оптимальної робочої пози з такими ергономічними характеристиками: ступні ніг - на підлозі або на підставці для ніг; стегна - в горизонтальній площині; передпліччя - вертикально; лікті - під кутом 70 - 90 град. до вертикальної площини; зап'ястя зігнуті під кутом не більше 20 град. відносно горизонтальної площини, нахил голови - 15 - 20 град. відносно вертикальної площини. У випадку, коли користування ПК є основним видом діяльності, то ПК і його периферійні пристрої (принтер, сканер тощо) розміщується на основному робочому столі з лівого боку. Висота робочої поверхні столу для ПК має бути в межах 680 - 800 мм, а ширина - забезпечувати можливість виконання операцій в зоні досяжності моторного поля. Він повинен мати простір для ніг висотою не менше 600 мм, шириною не менше 500 мм, глибиною на рівні колін не менше 450 мм, на рівні витягнутої ноги – не менше 650 мм.

Робоче сидіння (сидіння, стілець, крісло) користувача ПК повинно мати такі основні елементи: сидіння, спинку стаціонарні або знімні підлокітники.

Монітор та клавіатура мають розташовуватися на такій оптимальній відстані від очей користувача, але не повинні бути не ближче ніж 600 мм, з урахуванням розміру алфавітно-цифрових знаків та символів.

Неправильна організація робочого місця сприяє загальній і локальній напрузі м'язів шиї, тулуба, верхніх кінцівок, скривленню хребта й розвитку остеохондрозу.

В даному розділі проводиться аналіз середовища в якому розроблювався програмний продукт на основі санітарних норм України. Приміщення, в якому розроблявся програмний продукт розташоване на першому поверсі 10-поверхового будинку.

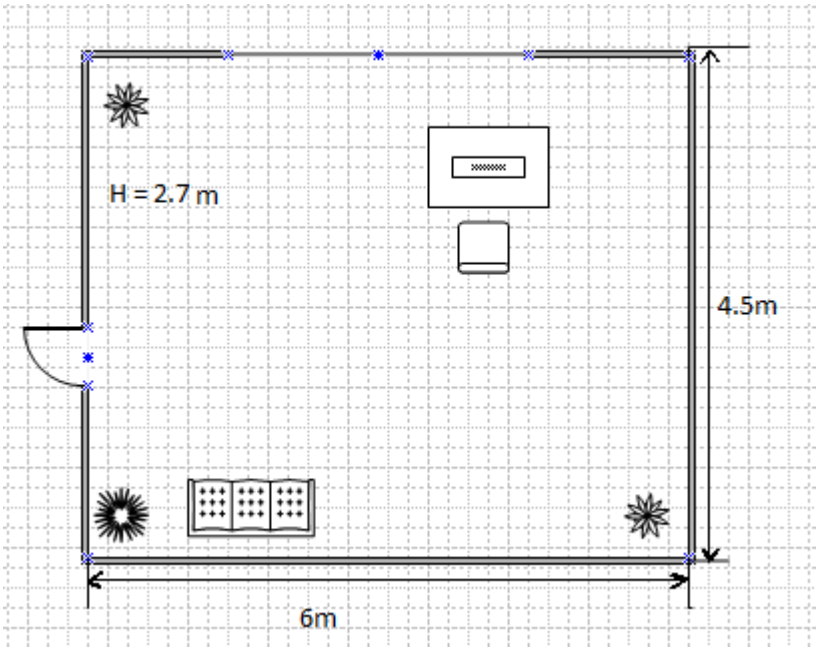

Рисунок 4.1 - План приміщення

Основні параметри приміщення наведені в таблиці 1.

Таблиця 4.1 - Геометричні параметри приміщення

Параметр приміщення	Значення
Довжина, м	6.00
Ширина, м	4.50
Висота, м	2.70
Площа, $м^2$	27.00
Об’єм, $м^3$	72.90

Розміщення принтера або іншого пристрою введення-виведення інформації на робочому місці має забезпечувати добру видимість монітору, зручність ручного керування пристроєм введення-виведення інформації в зоні досяжності моторного поля: по висоті 900 - 1300 мм, по глибині 400 - 500 мм.

Ергономіка робочого місця компанії Воля-Кабель повністю відповідає нормам.

Характеристики робочого місця відповідають нормативним вимогам у всьому НПАОП 0.00-1.28-10 та ДСанПіН 3.3.2-007-98).

Таблиця 4.2 - Порівняння фактичних і нормативних характеристик робочого місця

Параметр	Нормативне	Фактичне
Висота робочої	680-800 мм	700 мм
Глибина робочої	800-1000мм	900 мм
Висота сидіння над рівнем підлоги	400-500 мм	480 мм
Висота спинки стільця	300+/- 20 мм	320 мм
Регулювання нахилу спинки крісла	1-30°	1-30°
Глибина сидіння	400 мм та більше	450 мм
Висота простору для ніг	600 мм та більше	800 мм
Ширина простору для	500 мм та більше	520 мм
Глибина простору для	650 мм та більше	700 мм
Відстань від екрану до очей	600-700 мм	620 мм

4.2. Розрахунки освітлення та електричних приладів приміщення

4.2.1 Вимоги до освітлення

Відносно вікон робоче місце повинно бути розміщено так, щоб природне світло було збоку, переважно з лівого. Робоче місце, обладнане ПК повинно бути розташоване так, щоб уникнути попадання в очі прямого світла. Джерела штучного світла рекомендується розташувати з обох сторін від екрану паралельно напрямку зору. Вікна приміщень повинні мати регулювальні пристрої для відкривання. Як в приміщення джерелом світла є штучне освітлення, то застосовуватися, як правило, люмінесцентні лампи.

В приміщені знаходиться одне велике вікно з однієї сторони. Його характеристики:

Висота: L=1.5 м; ширина: W=3.5 м, то загальна площа одного вікна: $S=L*W=5$ м^2.

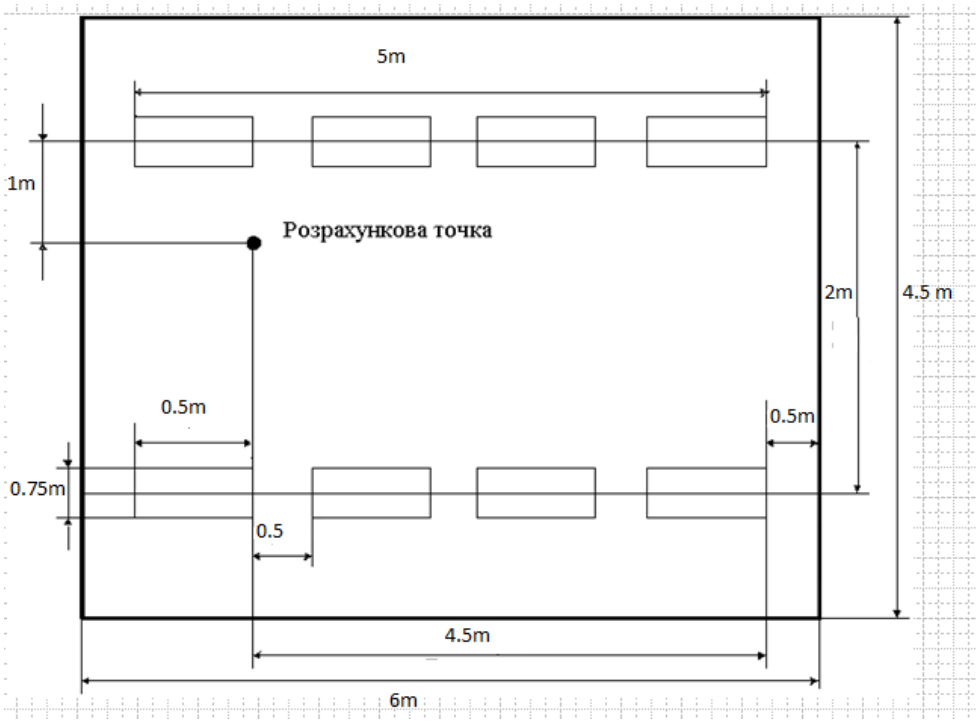

Рисунок 4.2 - Схема загального освітлення

Робота за дисплеєм ПЕОМ за розрядом зорових робіт відноситься до III розряду. При загальному висвітленні освітленість робочого місця повинна становити від 200 до 400 лк.

При штучному освітленні нормуються наступні параметри:

Е (лк) - найменша припустима освітленість;

М - показник дискомфорту;

Кп (%) - коефіцієнт пульсації освітленості;

Перевіримо, чи відповідають нормам фактичні параметри штучного освітлення в приміщенні. Номінальний світловий потік лампи білого світіння ЛБ-40.

$Ф_л$ = 3120 лм.

У приміщенні застосовуються світильники, у яких встановлені дві лампи.

Висоту підвісу світильника визначимо з формули :

$h = H - h_c - h_p - h_n$,

де

H - висота приміщення, м; h_c - висота світильника, м; h_n - відстань від стелі до підвісу, м; h_p - висота робочої поверхні, м.

Для розглянутого приміщення :

H = 2,7 м; h_c = 0,3 м; h_n = 0,3 м; h_p = 0.7 м.

звідси :

h = 2,7 - 0,3 – 0,3 – 0,7 = 1,4 м.

Світильники розташовані по 4 в 2 ряди. Відстань між рядами 2 метра, відстань від ряду до стіни 0,5 метра. Приміщення має наступні габарити:

довжина A = 6 метрів,

ширина B = 4,5 метрів.

Визначимо освітленість у робочій точці. Для розрахунку загальної рівномірної освітленості при горизонтальній робочій поверхні використаємо метод коефіцієнта використання світлового потоку.

Розрахункова формула для світлового потоку світильника має вигляд:

$$Ф_л = \frac{E \cdot K_з \cdot S \cdot Z}{N \cdot n},$$

де

N - число світильників у приміщенні, N = 4*2=8;

n - коефіцієнт використання світлового потоку;

$Ф_л$ - світловий потік ламп;

$K_з$ - коефіцієнт запасу, $K_з$ = 1.5;

Z - коефіцієнт нерівномірності;

S - площа приміщення;

Е - освітленість, створювана всіма світильниками.

Звідси одержуємо формулу для розрахунку освітленості на робочому місці:

$$E = \frac{Ф_л \cdot N \cdot n}{K_з \cdot S \cdot Z};$$

Коефіцієнт використання світлового потоку залежить від:

ККД, кривій розподілу сили світла світильника;

Коефіцієнта відбиття стелі Rc і стін Rc;

Висоти підвісу світильників $h_п$;

Показника приміщення і обчислимо за формулою:

$$i = \frac{A * B}{h * (A + B)};$$

i = (6 * 4,5) / (1,4 * (6 + 4.5)) = 1,64.

Нам відомо, що стеля й стіни пофарбовані в світло-сірий і світло-бежевий кольори. Приймаємо:

Rп = 50%, Rc = 30%.

Звідси: n = 42%.

$$E = \frac{3120 \cdot 8 \cdot 0{,}42}{1{,}4 \cdot 27 \cdot 1{,}1} = 254{,}75\ лк.$$

Виходячи з того, що по розряду зорової роботи робота за дисплеєм ПЕОМ відноситься до III розряду, тому при загальному освітленні освітленість робочого місця повинна становити від 200 до 400 лк. Фактична освітленість на робочому місці становить 254,75 лк. У такий спосіб для роботи з дисплеєм цілком достатньо існуючих джерел світла.

4.2.2 Мікрокліматичні умови

Мікроклімат робочих приміщень – це клімат внутрішнього середовища цих приміщень, що визначається діючої на організм людини з'єднанням температури, вологості, швидкості переміщення повітря.

Таблиця 4.3 - Значення мікроклімату

Період року	Параметр	Оптимальний	Фактичний
Теплий	Температура	23 – 25 °С	24-27 °С
	Вологість	40 – 60 %	40 %
	Швидкість повітря	≤ 0.1 м/с	
Холодний	Температура	22 – 24 °С	23-25 °С
	Вологість	40 – 60 %	50 %
	Швидкість повітря	≤ 0.1 м/с	

Всі показники задовольняють зазначеним вимогам для робіт категорії легка Іа і є задовільними для здоров’я людини. В приміщенні відсутні джерела шкідливих речовин. Спеціальні заходи з поліпшення або нормалізації цього параметру не потрібні. Умови мікроклімату у розглянутому приміщенні задовольняють вимогам встановленим у [11].

4.2.3. Захист від виробничого шуму й вібрацій

Для програмістів обчислювальних машин допустимі рівні звукового тиску та звуку на робочих місцях зазначені в таблиці 4.

Таблиця 5.3 - Допустимі рівні звукового тиску і рівні звуку для постійного широкополосного звуку

Допустимі рівні звукового тиску (дБ) в стандартизованих октавних смугах з середньогеометричними частотами, Гц	Допустимий рівень звуку, дБА

2	3	125	250	500	1000	2000	4000	8000	
6	1	61	54	49	45	42	40	38	50

В даному приміщенні джерелами шуму є лише вентилятори системного блоку ПК. По технічній документації сумарний шум не перевищує 32 дБА, що задовольняє нормативним вимогам.

Відстань від екрану монітора повинен складати 600-700 мм. Рівень ЕМ випромінювання повинен відповідати вимогам [12].

Джерелом ЕМ випромінювання в спектрі світлових та рентгенівських хвиль є монітор LG Flatron L1710S. Він є сертифікованим на Україні і відповідає умовам [13].

Захист досягається в результаті відповідної організації роботи, складення і дотримання графіку, при якому час контакту з джерелом випромінювання мінімальний, а продуктивність праці залишається на високому рівні.

4.3. Вимоги до безпеки

4.3.1. Вимоги електробезпеки

Технічні рішення із запобігання електотравм від контакту з нормально струмовідними елементами електроустаткування

- величина напруги мережі 380^{x}220В (міжфазна лінійна і фазна);
- всі нормально струмовідні елементів (в першу чергу електричні дроти) вкриті ізоляційними матеріалами;
- в джерелі безперебійного живлення персонального комп’ютера використовується механічне захисне блокування, що забезпечує вимикання напруги при його відкриванні;

- електромережа в приміщенні розведена в спеціальних каналах стін і підлоги.

Дане приміщення задовольняє вимоги до електробезпеки у приміщенні, в якому встановлені ЕОМ.

4.3.2. Пожежна безпека

Основні об’єкти та предмети горіння: обладнання, меблі, підлога, стіни, віконні та дверні рами, папір, тканини та інше.

Єдиною причиною виникнення пожежі в приміщенні (окрім підпалу— випадкового чи навмисного) може бути незадовільний стан електропристроїв та електропроводки. Робоче приміщення за вибухопожежною і пожежною небезпекою відноситься до приміщень категорії В, тому що у даному приміщенні містяться матеріали здатні при взаємодії з киснем повітря тільки горіти.

Клас приміщення з пожежонебезпеки — П-IIа, бо в приміщенні є тверді горючі речовини і матеріали.

4.3.3. Допомога при ураженні електричним струмом

Рятування життя людини, ураженої струмом залежить від швидкості і правильності дій осіб (колеги, працівники меду пункту підприємства, якщо такий є в наявності), що здійснюють допомогу. Передусім потрібно якнайшвидше звільнити потерпілого від дії електричного струму. Якщо неможливо відключити електричне обладнання від мережі, потрібно відразу приступити до звільнення потерпілого від струмопровідних частин, не доторкаючись при цьому до потерпілого.

Заходи долікарської допомоги після звільнення потерпілого залежать від його стану, її потрібно надавати негайно, по можливості на місці події, одночасно викликавши медичну допомогу. Якщо потерпілий не знепритомнів, потрібно забезпечити йому на деякий час спокій, не дозволяючи рухатись до прибуття лікаря. Якщо потерпілий дихає рідко і судорожно, але прослуховується пульс, потрібно негайно зробити йому штучне дихання. При відсутності

дихання, розширення зіниць і посиніння шкіри потрібно робити штучне дихання і непрямий масаж серця.

Надавати допомогу необхідно до прибуття лікаря, оскільки є багато випадків, коли штучне дихання і масаж серця повертали потерпілих до життя.

4.4. Висновки

Приведені рекомендації щодо організації робочого місця на підприємстві дозволяють підвищити рівень безпеки праці, попередити виникнення надзвичайних ситуацій та надати першу медичну допомогу при виникненні надзвичайної ситуації. Служби охорони праці, а саме відповідні служби і структурні підрозділи підприємства повинні здійснювати постійний контроль за виконанням робіт у відповідності з вимогами з охорони праці, електро-, газо- і пожежобезпеки, не допускати до роботи осіб, які не пройшли інструктаж та не здали заліки по питаннях охорони праці. Роботодавець повинен впроваджувати сучасні засоби техніки безпеки, які запобігають виробничому травматизмові, і забезпечувати санітарно-гігієнічні умови, що запобігають виникненню професійних захворювань працівників.

Перед початком роботи слід переконатися у справності електропроводки, вимикачів, штепсельних розеток, за допомогою яких обладнання включається в мережу, наявності заземлення комп'ютера, його працездатності,

Щоб уникнути пошкодження ізоляції проводів і виникнення коротких замикань не дозволяється: вішати що-небудь на дроти, зафарбовувати й білити шнури і дроти, закладати дроти і шнури за газові та водопровідні труби, за батареї опалювальної системи, висмикувати штепсельну вилку з розетки за шнур, зусилля повинне бути додане до корпусу вилки.

Для виключення ураження електричним струмом забороняється: часто вмикати і вимикати комп'ютер без необхідності, торкатися до екрану і до тильної сторони блоків комп'ютера, працювати мокрими руками, працювати на засобах обчислювальної техніки та периферійному обладнанні, що мають порушення

цілісності корпусу, порушення ізоляції проводів, несправну індикацію включення живлення, з ознаками електричної напруги на корпусі, класти на обладнання сторонні предмети.

Забороняється під напругою очищати від пилу і забруднення електрообладнання. Забороняється перевіряти працездатність електроустаткування в непристосованих для експлуатації приміщеннях з струмопровідними підлогами, сирих, не дозволяючих заземлити доступні металеві частини. Неприпустимо під напругою проводити ремонт засобів обчислювальної техніки і периферійного обладнання. Ремонт електроапаратури проводиться тільки фахівцями-техніками з дотриманням необхідних технічних вимог.

Після закінчення роботи необхідно знеструмити всі засоби обчислювальної техніки і периферійне устаткування. У разі безперервного виробничого процесу необхідно залишити включеними тільки необхідне обладнання.

ВИСНОВКИ

Отже, в ході даного проекту було запропоновано концепції для системи управління розумним домом, а саме: управління електроенергією, контроль доступу, перевірка присутності тощо. Також було визначено схему потоків даних, потенційні вразливі місця та засоби захисту. Була запропонована криптографічна схема на основі сукупності PKI та Base64, яка за умов справної роботи сервера та його надійності, являється практично невразливою. Виходячи з матеріалу, можна зробити ще ряд висновків.

Сьогодні, напевно, ніхто не зможе з упевненістю назвати точну цифру сумарних втрат від комп'ютерних злочинів, пов'язаних з несанкціонованих доступом до інформації. Це пояснюється, насамперед, небажанням постраждалих компаній оприлюднювати інформацію про свої втрати, а також тим, що не завжди втрати від розкрадання інформації можна точно оцінити в грошовому еквіваленті.

Причин активізації комп'ютерних злочинів і пов'язаних з ними фінансових втрат досить багато, істотними з них є:

- Перехід від традиційної "паперової" технології зберігання і передачі відомостей на електронну і недостатнє при цьому розвиток технології захисту інформації в таких технологіях;
- Об'єднання обчислювальних систем, створення глобальних мереж і розширення доступу до інформаційних ресурсів;
- Збільшення складності програмних засобів і пов'язане з цим зменшення їх надійності та збільшенням числа вразливостей.
- Комп'ютерні мережі, в силу своєї специфіки, просто не зможуть нормально функціонувати і розвиватися, ігноруючи проблеми захисту інформації.

Для того щоб спрогнозувати напрямок розвитку технології, проаналізуємо доступні нам факти. Концепція «розумного будинку» цікава і перспективна. На даний момент велика кількість компаній, в тому числі в Росії, пропонують

послуги зі створення таких диво-будинків. Сама технологія реалізується дешево (безпровідно або з використанням існуючих силових кабелів), а ось настройка такої системи, особливо якщо вона управляється програмно з комп'ютера, - річ досить складна для обивателя, як і будь-які нові технології, до яких люди довго звикають, і обійдеться не так вже й дешево її власникам. Крім того, наявність ряду таких рішень необхідно враховувати при розробці дизайну приміщень. Ідеальне місце застосування таких технологій - приватні будинки і котеджі, а також великі офіси. В принципі, враховуючи, що власники заміських будинків витрачають великі гроші на їх утримання, вартість такого рішення буде відносно невеликою.

У розумному будинку вся електроніка і побутова техніка - від кліматичних систем до телевізорів - управляється надзвичайно складними комп'ютерними системами. «Розумний будинок» включає світло і музику, коли гості і близькі входять в будинок і переміщуються по численних кімнатах. При цьому світлове та музичний супровід у міру пересування відвідувача по «розумним» апартаментів змінюється відповідно до побажань господаря, які збережені в налаштуваннях. Людині не потрібно задавати температурний режим в приміщеннях або налаштовувати освітлення - встановлена «інтелектуальна» система станом господаря розпізнає, яка температура і освітлення необхідні йому в даний момент для повного комфорту. Для забезпечення зручності в квартирі можуть використовуватися різноманітні технології, починаючи від саморобних пристроїв і закінчуючи високоінтелектуальними комп'ютерними АСУ.

ПЕРЕЛІК ПОСИЛАНЬ

1. Е.А. Тесля. «Умный дом» своими руками. Строим интеллектуальную цифровую систему в своей квартире / Е.А. Тесля – Санкт Петербург, 2008. – 224с.
2. Т. Р. Элсенпитер, Дж. Велт. «Умный Дом строим сами» / Т. Р . Элсенпитер, Дж Велт/ КУДИЦ-ОБРАЗ. 2005. – 384с.
3. В.Н. Харке «Умный дом. Объединение в сеть бытовой техники и систем коммуникаций в жилищном строительстве» / В.Н. Харке– М.: Техносфера, 2006. – 292с.
4. М. Э. Сопер. Практические советы и решения по созданию « Умного дома » / М. Э. Сопер. – М.: НТ Пресс, 2007. – 432 с.
5. Т. Р. Элсенпитер, Дж. Велт. «Умный Дом строим сами» / Т. Р.Элсенпитер, Дж Велт / КУДИЦ-ОБРАЗ. 2005. – 384с.
6. В.Н. Гололобов. «Умный дом» своими руками. / В.Н. Гололобов – М.: НТ Пресс, 2007. – 416 с.
7. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия. - М.: Изд-во "Интернет-университет информационных технологий - ИНТУИТ.ру", 2005. - 608 с.: ил.
8. Ярочкин В.И. Информационная безопасность. - М.: Изд-во "Академический проект", 2004. - 640 с.
9. Бармен С. Разработка правил информационной безопасности. - М.:
10. Mark Gasson, Martin Meints, Kevin Warwick (2005), D3.2: A study on PKI and biometrics, FIDIS deliverable (3)2, July 2005
11. Санітарні норми мікроклімату виробничих приміщень: ДСН 3.3.6.042-99.
12. Государственные санитарные правила и нормы работы с визуальными дисплейными терминалами электронно-вычислительных машин: ДСанПіН 3.3.2.007-98.

13. НПАОП 0.00-1.28-10 “Правила охорони праці під час експлуатації ЕОМ” – Держгірпромнагляд, № 65 від 26 березня 2010 р.
14. Природнє і штучне освітлення: ДБН В.2.5-28-2006.
15. Санітарні норми виробничого шуму, ультразвуку та інфразвуку: ДСН 3.3.6.037-99-2000.
16. «Санитарные правила работы с источниками неиспользуемого рентгеновского излучения». № 1960-79. - М.: «Атомиздат», 1981. -32 с.
17. Правила безпечної експлуатації електроустановок споживачів, затверджених наказом Комітету по нагляду за охороною праці Міністерства праці та соціальної політики України від 09 січня 1998 року № 4, зареєстрованих у Міністерстві юстиції України 10 лютого 1998 року за № 93/2533 (НПАОП 40.1-1.21-98)
18. НАПБ Б.03.002-2007 Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та журнал „Бизнес и безопасность” № 1/2008)
19. Правила пожежної безпеки в Україні, затверджених наказом МНС України від 19.10.2004 № 126, зареєстрованих в Міністерстві юстиції України 4.11.2004 за № 1410/10009 (НАПБ А.01.001 - 04).