**Список використаних джерел**

1. https://esp8266.ru/ [Електронний ресурс] - спільнота розробників
2. https://hobbytech.com.ua/%D0%B7%D0%BD%D0%B0%D0%BA%D0%BE%D0%BC%D0%B8%D0%BC%D1%81%D1%8F-%D1%81-%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D0%B5%D0%BC-esp8266-%D0%BF%D0%BE%D0%B4%D1%80%D0%BE%D0%B1%D0%BD%D0%B5%D0%B5/ - знайомство з ESP8266
3. https://arduino-kit.ru/blogs/blog/smart_home_projects [Електронний ресурс] - приклади проектів та підключаємих модулів
4. https://ru.wikipedia.org/wiki/ESP8266 [Електронний ресурс] - загальна інформація про мікроконтроллер
5. https://habr.com/ru/post/394535/ [Електронний ресурс] - с чого почати роботу з мікроконтроллером

---

УДК 004.056.55

# ОРГАНІЗАЦІЙНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

**Сідлецький Є. В.,** студ. гр. КБ-161
Науковий керівник: **Петренко Т. А.,** ст. викладач кафедри
кібербезпеки та математичного моделювання
*Національний університет «Чернігівська політехніка»*

В сучасному світі ми використовуємо інформаційні технології у всіх сферах нашого життя, що дає нам можливість з легкістю виконати поставлене перед нами завдання, знайти потрібну нам інформацію, тим самим спростити наше життя. Велике питання постає щодо захисту інформації, інформаційних ресурсів та каналів передачі даних від злочинних дій зловмисників. В період розвитку інформаційних технологій електронних платежів та документообігу існують застереження щодо втручання сторонніми особами, з метою завдання шкоди підприємству, що може призвести до збитків.

Мета моєї доповіді - дослідити організаційні засоби захисту інформації в системах електронного документообігу. Організаційні засоби - це організаційно-технічні і організаційно-правові заходи, реалізовані в процесі створення і експлуатації IT-обладнання, телекомунікаційного обладнання для забезпечення захисту інформації. Організаційні методи захисту інформації включають заходи та дії, які повинні робити керівники під час створення і експлуатації системи, щоб гарантувати певний рівень інформаційної безпеки.

Спираючись на закони та нормативно-правові акти на підприємствах та відомствах, незалежно від форми власності, створюють спеціальні служби для забезпечення захисту інформації на підприємстві, які безпосередньо підпорядковуються керівництву організації. Керівники відділу забезпечують створення та функціонування системи з захисту інформації на підприємстві. Повну відповідальність за стан інформаційної безпеки несуть керівники організації.

На організаційному рівні вирішуються наступні завдання забезпечення безпеки інформації в системи:

Завдання забезпечення безпеки інформації в системі

- обмеження доступу на об'єкт і до ресурсів системи;
- виховання й навчання обслуговуючого персоналу й користувачів;
- удосконалювання системи захисту інформації;
- організація робіт з розробки системи захисту інформації;
- оцінка ефективності функціонування системи захисту інформації;
- контроль виконання встановлених правил роботи в системи.

Основні властивості методів і засобів організаційного захисту:

- Введеняя обмеження фізичного доступу до об'єктів захисту;
- обмеження можливості перехоплення ПЕМВН;
- розмежування прав доступу до інформаційних ресурсів та здійснення шифрування інформації при її зберіганні і передачі, виявлення та знищення апаратних і програмних закладок;
- виконувати резервне копіювання документів;
- проводити профілактику зараження комп'ютерними вірусами.

Регламент документообігу являє собою сукупність правил інформаційної діяльності суб'єктів інформаційних відносин, визначених законодавством, нормативними актами або угодами. Регламент документообігу визначає ролі та права суб'єктів щодо створення, володіння, користування та розпорядження документами, порядок оформлення і фіксації інформації на носієві інформації.

Відповідно до статті 6 Закону України «Про електронні документи та електронний документообіг»[1] електронний підпис є обов'язковим реквізитом електронного документу (ЕД), який використовується для ідентифікації автора та/або підписувача ЕД іншими суб'єктами електронного документообігу.

Статтею 1 Закону України "Про електронний цифровий підпис"[2] визначено такі терміни:

- електронний підпис – дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних;

- електронний цифровий підпис (ЕЦП) – вид електронного підпису, отриманого за результатом криптографічного перетворення наборі електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа;

Для забезпечення захисту інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах повинні обов'язково виконуватися наступні процедури:

– автентифікація – процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора;

– ідентифікація – процедура розпізнавання користувача в системі, як правило за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою.

Більш того, організація захисту інформації електронної системи документообігу потребує додаткову увагу на забезпечення доступності публічної інформації та блокування несанкціонованого доступу. Найбільш незахищене місце при організації захисту системи електронного документообігу – це діяльність користувачів, а не технічно-апаратні засоби захисту інформації. Відразу як документ потрапляє до користувача, конфіденційність цього документа може бути порушена. Він має безліч способів як скористатися інформацією, можливе копіювання на пристрої зовнішнього типу, або просте фотографування документу, і тоді він втрачає свою цілісність.

Реєстрація дій користувача є важливою точкою захисту для електронного документообігу. Його правильна реалізація в системі дозволяє відстежувати всі незаконні дії і знаходити несправності, а при негайному втручанні навіть зупиняти спроби незаконних або шкідливих дій. Такі методи реалізовані в системі електронного документообігу DIRECTUM. DIRECTUM - це система електронного документообігу, спрямована на підвищення ефективності роботи всіх фахівців організацій в різних сферах їх діяльності.

Система DIRECTUM підтримує повний життєвий цикл управління документами, при цьому традиційне «паперове» діловодство органічно вписується в електронний документообіг. DIRECTUM забезпечує ефективну організацію і контроль ділових - узгодження документів, обробка складних замовлень, підготовка і проведення нарад, підтримка циклу продажів і інших процесів взаємодії. В системі виконується багато циклів,

насамперед, створення і зберігання різних неструктурованих документів, підтримка версій документів і ЕЦП; структурування документів по папках; призначення прав доступу на документи; історія роботи з документами; повнотекстовий і атрибутивний пошук документів; підтримка процесів узгодження і обробки документів на всіх стадіях їх життєвого циклу; видача електронних завдань і контроль їх виконання; взаємодія між співробітниками в ході бізнес-процесів; підтримка вільних і жорстких маршрутів.[3]

Підхід до захисту електронного документообігу повинен бути комплексним. Треба тверезо оцінити потенційні загрози і ризики системи електронного документообігу та ступінь потенційних втрат від загроз. Захист системи електронного документообігу не зводиться до захисту документів і обмеження доступу до них. Захист системного обладнання, комп'ютерів, принтерів та інших пристроїв є важливим завданням, захист мережного середовища, в якій працює система, захист каналів передачі даних і мережевих пристроїв.

Комплекс організаційних заходів відіграє важливу роль на кожному рівні захисту. Погана організація може звести нанівець всі технічні дії, незалежно від того, наскільки вони досконалі. При виборі засобів захисту слід оцінити реальні втрати від розкриття або спотворення інформації і порівняти з вартістю засобів захисту [4]. Але будь-якому випадку слід вводити елементарні, найдешевші і не менш ефективні засоби - вхід в систему управління документами повинен здійснюватися через систему паролів з розмежованими рівнями доступу. Фізичний доступ в приміщення, де встановлена система управління електронним документообігом, повинен здійснюватися відповідно до внутрішніх правил та бути обмежений стороннім особам.

**Список використаних джерел**

1. Про електронні документи та електронний документообіг [Електронний ресурс] – Режим доступу: URL: http://zakon1.rada.gov.ua/laws/show/851-15
2. Про електронний цифровий підпис [Електронний ресурс] – Режим доступу: URL: http://zakon2.rada.gov.ua/laws/show/852-15/
3. DIRECTUM - [Електронний ресурс]: – Режим доступу: URL: https://ru.wikipedia.org/wiki/Directum
4. ЗАХИСТ ІНФОРМАЦІЇ В ЕЛЕКТРОННОМУ ДОКУМЕНТООБІГУ [Електронний ресурс] – Режим доступу: URL: http://elartu.tntu.edu.ua/bitstream/lib/23058/2/CAZST_2017v2_Zavodyanskiy_V_O-Protection_of_information_65-66.pdf

---

УДК 004.056.55

## АНАЛІЗ СКЛАДОВИХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

**Коротка Г. М.,** студ. гр. КБ-161,
**Петренко Т. А.,** доцент кафедри кібербезпеки та математичного моделювання
*Національний університет «Чернігівська політехніка»*

Всі підприємства, незалежно від форми власності, масштабів та сфери діяльності, створюють, опрацьовують та зберігають документи. Організація системи електронного документообігу (СЕД) – дієвий сучасний процес документообігу, що дозволяє оптимізувати роботу компанії. Електронні документи можуть одночасно використовуватися співробітниками в рамках однієї робочої групи, відділу або всього підприємства. На відміну від паперового документообігу, де процес одержання доступу до документів може тривати декілька хвилин, годин, днів, а іноді і тижнів, доступ до електронних документів здійснюється за декілька секунд. Використовуючи СЕД, будь-яка організація зможе заощаджувати свій робочий час та приймати оперативні рі

шення в декілька разів швидше.