Секція 4

КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА КІБЕРБЕЗПЕКА

КІБЕРБЕЗПЕКА ТА КІБЕРЗАХИСТ ЯК СКЛАДОВІ СИСТЕМИ ЗАХИСТУ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Василенко Д.О., здоб. ОС «магістр»
Науковий керівник – канд. екон. наук, доц. **Г.С. Морозова**
Державний біотехнологічний університет

Комп'ютерна інформація стала надзвичайно важливою в сучасному світі. Вона зберігається на комп'ютерах, серверах та в хмарних обчисленнях і використовується в багатьох галузях, таких як фінанси, здоров'я, освіта, промисловість та інші.

Кібербезпека та кіберзахист є важливими складовими системи захисту національної безпеки. Кібератаки можуть завдати значної шкоди державним структурам, економіці, інфраструктурі та іншим важливим секторам.

Забезпечення кібербезпеки та кіберзахисту національних інформаційних систем та критично важливих інфраструктур є надзвичайно важливим завданням для держави. Для цього потрібна ефективна стратегія та плани дій, включаючи регулярне оновлення кібербезпекових заходів та забезпечення відповідного рівня кіберзахисту. Недостатня захищеність може призвести до втрати даних, порушення законодавства про захист персональних даних та збитків для бізнесу і репутації компаній. Тому важливо розуміти роль кібербезпеки та приділяти достатню увагу захисту комп'ютерної інформації.

Кібербезпека – це сукупність заходів, які приймаються для захисту комп'ютерних систем, мереж і даних від несанкціонованого доступу, зламів, вірусів та інших загроз. Роль кібербезпеки полягає в розробці, впровадженні та підтримці захисних заходів, які допоможуть уникнути кібератак, збільшити надійність та безпеку інформаційних систем та мереж.

Кібератака – це несанкціоновані дії зловмисників, які намагаються використати уразливості комп'ютерних систем та мереж для здійснення атаки, щоб отримати незаконний доступ до комп'ютерної інформації або завдати шкоди системі.

Віруси та програми-шпигуни – це програми, які вбудовуються в комп'ютерну систему та мережу, з метою отримання доступу до інформації або зіпсувати роботу системи.

Фішинг – це метод, який використовується для отримання конфіденційної інформації, такої як логіни та паролі, шляхом виманювання користувачів на підроблені веб-сторінки або електронні листи.

DDoS-атаки – це атаки, які спрямовані на перевантаження мережі або сервера надмірним потоком трафіку, що призводить до затримок у роботі системи або навіть до її падіння.

Вторгнення – це атаки, які полягають у зламі системи або мережі, з метою отримання незаконного доступу до комп'ютерної інформації або зіпсування роботи системи.

Крадіжка даних – це викрадення конфіденційної інформації шляхом зламу системи або мережі.

Для захисту від кібератак необхідно застосовувати різноманітні заходи кібербезпеки, такі як встановлення міцних паролів, шифрування даних, використання програмного забезпечення для виявлення вторгнень, забезпечення регулярних оновлень програмного забезпечення та жорсткого забезпечення, здійснення резервного копіювання даних та інші. Для успішного захисту необхідно постійно моніторити стан безпеки та здійснювати регулярні перевірки та оновлення.

Розробка безпечного програмного забезпечення є надзвичайно важливою для запобігання кібератак та збільшення надійності комп'ютерних систем. При розробці програмного забезпечення потрібно враховувати можливість злому та використання програмних помилок. Недостатній захист програм може призвести до злому, викрадення даних та порушення безпеки.

Для розробки безпечного програмного забезпечення потрібно використовувати найкращі практики безпеки та стандарти, такі як Secure Software Development Life Cycle (SSDLC) та Open Web Application Security Project (OWASP). Ці підходи допомагають забезпечити безпеку на кожному етапі розробки програмного забезпечення, включаючи проектування, розробку, тестування та випуск програм.

Розробка безпечного програмного забезпечення знижує ризик кібератак та збільшує надійність комп'ютерних систем. Компанії, які розуміють значення безпеки та приділяють достатню увагу розробці безпечного програмного забезпечення, мають менше шансів стати жертвою кібератак та втратити довіру своїх клієнтів. Безпека повинна бути увімкнена на всіх етапах проектування та розробки, а не додаватись на пізніших етапах, коли це може бути надто пізно.

Шифрування – це процес перетворення звичайного тексту в кодований шифртекст, що може бути розшифрований лише з використанням спеціального ключа. Шифрування та інші методи забезпечення конфіденційності даних є важливими для захисту інформації в інформаційних системах.

Одним з основних методів шифрування є симетричне шифрування, де один ключ використовується для шифрування та розшифрування даних. Але цей метод має недоліки, оскільки ключ повинен бути переданий з однієї сторони до іншої, що може бути небезпечним, якщо зловмисник отримує доступ до ключа.

Іншим методом шифрування є асиметричне шифрування, де використовуються два ключі: публічний та приватний. Публічний ключ відкритий для всіх, але зашифровані повідомлення можуть бути розшифровані

лише з використанням приватного ключа. Цей метод забезпечує більшу безпеку, оскільки приватний ключ залишається в таємниці.

Крім шифрування, інші методи забезпечення конфіденційності даних включають контроль доступу та аутентифікацію. Контроль доступу забезпечує, що лише авторизовані користувачі мають доступ до інформації, а аутентифікація визначає, що користувач є тим, за кого він себе видає.

Застосування шифрування та інших методів забезпечення конфіденційності даних є важливим для захисту конфіденційної інформації в інформаційних системах, що може бути вкрадена або використана зловмисниками. Ці методи є необхідними для забезпечення надійного зберігання та передачі конфіденційної інформації через інформаційні системи.

Шифрування забезпечує захист від перехоплення та читання даних зловмисниками, а інші методи, такі як контроль доступу та аутентифікація користувачів, забезпечують захист від несанкціонованого доступу до цієї інформації. Важливо також пам'ятати, що шифрування та інші методи забезпечення конфіденційності даних повинні бути поєднані з іншими методами кібербезпеки, такими як моніторинг систем та виявлення вразливостей, для забезпечення повного захисту від кібератак.

Кібербезпека стикається з численними викликами, які постійно змінюються та вдосконалюються зловмисниками.

До основних викликів кібербезпеки можна віднести:

1. Розвиток нових технологій та зростання кількості підключених до мережі пристроїв, що збільшує кількість вразливих точок для кібератак.
2. Зростання складності кібератак та поява нових видів загроз, таких як атаки на штучний інтелект та інтернет речей.
3. Недостатня увага до кібербезпеки з боку користувачів та компаній, що може призвести до появи нових вразливостей та атак.
4. Брак кваліфікованих кадрів у галузі кібербезпеки, що призводить до складнощів у виявленні та реагуванні на кібератаки.

Для розв'язання цих проблем можуть використовуватися такі можливості:

1. Розробка нових методів та алгоритмів кібербезпеки, що дозволяють ефективніше виявляти та запобігати кібератакам.
2. Забезпечення навчання та підвищення кваліфікації персоналу з питань кібербезпеки.
3. Впровадження культури кібербезпеки серед користувачів та компаній, що дозволить зменшити кількість вразливих точок та ризиків для кібератак.
4. Співпраця між державними та приватними організаціями для розробки та впровадження стратегій кібербезпеки на рівні держави та галузі.

Інформаційні джерела:

1. Кібергігієна. Кібербезпека. Безпека держави : матеріали наукових семінарів (Київ, 27 листопада 2020 р.) / відп. ред. А. М. Десятко. – Київ : Київ. нац. торг.-екон. ун-т, 2020. – 101 с.

2. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. К.: Видавничий дім «Кондор», 2019. — 272 с.

3. Кібербезпека в сучасному світі : матеріали II Всеукраїнської науково-практичної конференції (м. Одеса, 20 листопада 2020 р.) / за ред. О. В. Дикого ; уклад.: Н. І. Логінова, В. Д. Бойко, М. О. Флюнт. – Одеса : Видавничий дім «Гельветика», 2020. – 244 с.

4. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К. , 2018. – 320 с

5. Закон України «Про основні засади забезпечення кібербезпеки України (Відомості Верховної Ради (ВВР) , 2017, № 45, ст.403)

ВИЗНАЧЕННЯ ВИМОГ ДО СИСТЕМИ АВТОМАТИЗАЦІЇ ПРОЦЕСУ ПРИГОТУВАННЯ І РОЗДАЧІ КОРМІВ НА СВИНОФЕРМІ

Глєбов Д.В., здоб. ОС «магістр»
Науковий керівник – канд. техн. наук, доц. **І.Г. Абраменко**
Державний біотехнологічний університет

Автоматизація сільськогосподарського виробництва підвищує надійність і продовжує термін служби устаткування, полегшує й оздоровлює умови праці, підвищує безпеку праці й робить її більш комфортною, скорочуються використання робочої сили й економічні витрати, збільшується кількість і якість продукції. Автоматизація в сільському господарстві має свої особливості. Основні технологічні процеси виробництва сільськогосподарської продукції пов'язані з біологічними процесами.

Схему керування приготуванням і роздачею кормів можна реалізувати як на підставі релейно-контактної схеми, так і на базі контролера. Більш раціональним є реалізація на базі контролера, що обумовлене наступними факторами:

– надійність – виключення зі схеми великої кількості релейно-контактних елементів і регуляторів, що підвищує надійність і дозволяє простіше усувати неполадки (скорочує можливі місця їх появи);

– простота виконання (зручний і доступний інтерфейс контролера дозволяє реалізовувати на ньому необхідні завдання при мінімумі зусиль);

– можливість моніторингу (контролер дозволяє виконувати контроль і моніторинг виконуваного процесу в режимі реального часу);

– функціональність (у випадку зміни технологічного процесу (часу спрацьовування, затримок, черговості виконуваних процесів, уставок), можна обійтися без впровадження нових елементів схеми шляхом перепрограмування контролера);

– економічна доцільність (вартість нижче вартості апаратури, використовуваної без застосування контролера. У багатьох випадках, застосування контролерів, не вимагає наявності постійного обслуговуючого персоналу).

Схема керування повинна забезпечити роботу системи в автоматичному й налагоджувальному режимах і технологічну сигналізацію про роботу