онлайн ринків ЄС для українських споживачів та бізнесу, цифрові інноваційні продукти та послуги, посилення захисту прав споживачів в Інтернеті, зниження транзакційних витрат для бізнесу, підвищення якості та прозорості державних цифрових послуг та електронного урядування, а також інтенсифікація інноваційного розвитку в Україні.[3]

Водночас інтеграція України до ЄЦР тягне за собою низку зобов'язань: узгодити національне законодавство та стандарти із законодавством і стандартами ЄС; забезпечити інституційну та технічну спроможність, а також інтероперабельність цифрових систем. Для бізнесу в Україні це означає зіткнення з новими вимогами ЄС, спрямованими на покращення захисту прав споживачів та персональних даних, а також посилення конкуренції з боку європейських компаній на цифрових ринках. Однак ці зміни необхідні, якщо країна хоче побудувати спільний економічний простір з ЄС, особливо з огляду на зростаючий вплив цифрових технологій на міжнародну економіку.

Інформаційні джерела:

1. Стратегія інтеграції України до Єдиного цифрового ринку Європейського Союзу («Дорожня карта»). URL : https://docs.google.com/document.

2. EU Digital Single Market Aspects. Department of Enterprise, Trade and Employment, Dublin, 2023. URL:https://enterprise.gov.ie/

3. European commission: Association Implementation Report on Ukraine: Brussels, URL: https://www.eeas.europa.eu/sites/default/files/documents.

КІБЕРБЕЗПЕКА КОМП'ЮТЕРНИХ СИСТЕМ АГРОПРОМИСЛОВОГО КОМПЛЕКСУ

Петренко М.В., здоб. вищої освіти
Закутний В. М., здоб. вищої освіти
Піскачова І.В., канд. техн. наук, снс
Державний біотехнологічний університет

Зараз, з наявними тенденціями в галузі розвитку науки і техніки, з'явилася можливість впровадження автоматизації виробництва агропромислового комплексу (АПК), роблячи його конкурентоспроможними в умовах сучасного ринку. Автоматизація виробничих процесів однозначно призводить до підвищення продуктивності праці та підприємства загалом, поліпшення якості продукції, а також підвищення рівня безпеки на виробництві. Напрямок діяльності людини в умовах автоматизації зміщується на обслуговування виробничих процесів і контроль системи, а також на аналіз діяльності підприємства.

Сьогодні цифрові технології охоплюють більшість виробництв в сільському господарстві Цифрові технології можуть надавати змогу контролювати повний цикл рослинництва чи тваринництва, «розумні» пристрої вимірюють і передають параметри ґрунту, рослин, мікроклімату тощо. Усі ці дані з датчиків, дронів та іншої техніки аналізуються спеціальними

програмами. Мобільні або онлайн-додатки приходять на допомогу фермерам і агрономам, щоб визначити сприятливий час для посадки або збору врожаю, розрахувати схему добрив, спрогнозувати врожай і багато іншого. Приблизно 70% фермерських господарств США, Канади та Європи вже використовують «розумні» технології для сільського господарства.

Серед технологій, які впроваджені та можуть бути впроваджені в українському АПК, це програмні комплекси для управління фермами, роботизовані системи, безпілотники для моніторингу об'єктів сільського господарства, технології точного землеробства на базі інтернету речей. Однак для отримання максимального ефекту важливо впроваджувати не лише окрему «розумну» техніку, а й комплексні рішення для автоматизації процесів в агропромисловому комплексі. Зокрема, аграріям та фермерам необхідно переходити до раціонального використання добрив, виходячи з потреб конкретного поля. Так звана «цифрова карта» сільськогосподарських земель виконана на основі даних хімічного аналізу ґрунтів. Враховуючи стан ґрунту, аграріям дають рекомендації щодо оптимальної посадки сільськогосподарських культур, кількості та виду добрив та засобів захисту рослин. Тоді «розумна» сільськогосподарська техніка – сівалки, обприскувачі, розкидачі отримують карту завдань. Можна буде керувати цими процесами через веб-інтерфейс або в мобільному додатку, де відображаються всі створені системою журнали полів і рекомендації, а повідомлення на мобільному телефоні будуть нагадувати про виконання певних робіт вчасно.

Інформація, що пов’язана з АПК, у своїй більшості, є конфіденційною. Тому захист цієї інформації при обробці та передаванні лініями зв’язку є актуальною задачею.

Криптографія – наука, яка вивчає способи створення та застосування секретних кодів. Використання криптографії – один з поширених методів, що значно підвищують безпеку передачі даних в мережах ЕОМ і при обміні інформацією між віддаленими об'єктами. Для перетворення (шифрування) інформаційних повідомлень зазвичай використовується певний алгоритм або пристрій, що реалізує заданий алгоритм, які можуть бути відомі широкому колу осіб. Управління процесом шифрування здійснюється за допомогою періодично змінюваного коду ключа, що забезпечує кожен раз оригінальне представлення інформації при використанні одного і того ж алгоритму або пристрою. Знання ключа дозволяє просто і надійно розшифрувати текст. В іншому випадку ця процедура може бути практично нездійсненна навіть при відомому алгоритмі шифрування.

Класифікація методів шифрування (криптоалгоритмів) може бути здійснена за такими ознаками:

- за типом ключів (симетричні криптоалгоритми, асиметричні криптоалгоритми);
- за розміром блоку інформації (потокові шифри, блокові шифри);
- за характером впливів, що здійснюються над даними (метод заміни (перестановки), метод підстановки, аналітичні методи, адитивні методи (гамування), комбіновані методи) та ін.

Кодування може бути смислове, символьне, комбіноване.

Для захисту інформації в АПК не потребуються складні та дорогі методи шифрування, можна використовувати прості але добре опрацьовані методи. До таких методів відносяться методи симетричного шифрування. У симетричних криптоалгоритмах для шифрування та дешифрування повідомлення використовується один і той же блок інформації – ключ, який повинен зберігатися в таємниці і передаватися способом, що виключає його перехоплення. Використання одного ключа для обох операцій робить процес простим. Просте перетворення інформації служить досить ефективним засобом, що дає можливість приховати її сенс від більшості не дуже кваліфікованих порушників.

Дуже прості методи перестановки добре опрацьовані і є класичними, характеризуються короткою довжиною ключа, а надійність їх захисту визначається складністю алгоритмів перетворення. Ці методи теж відносяться до симетричного шифрування. Шифри перестановок зараз у чистому вигляді не використовують, оскільки їхня криптостійкість недостатня.

Більшей криптостійкістю серед простих симетричних систем шифрування володіє система Віженера. Вона є самою найстаршою з багатоалфавітних систем, у якої ключ - слово чи фраза.

Американський стандарт криптографічного закриття даних DES (Data Encryption Standard), ухвалений у 1978 р., був типовим представником сімейства блокових шифрів і одним із найпоширеніших криптографічних стандартів на шифрування даних, що застосовуються у США. Цей шифр допускає ефективну апаратну і програмну реалізацію, причому можливе досягнення швидкостей шифрування до декількох мегабайт на секунду. Спочатку метод, що лежить в основі цього стандарту, був розроблений фірмою IBM для своїх цілей. Його перевірило Агентство Національної Безпеки США, яке не виявило в ньому статистичних або математичних вад. DES має блоки по 64 біт і ґрунтується на 16-кратній перестановці даних, також для шифрування використовує ключ у 56 біт.

Найбільш просунутим серед блокових симетричних систем є AES (Advanced Encryption Standard), що являє собою алгоритм, що не використовує мережі Фейстеля. AES – симетричний ітеративний блоковий алгоритм; базується на принципах нової мережі підстановок-перестановок. Має архітектуру квадрат, для якої характерно:

– представлення блоку, що шифрується, у вигляді двовимірного байтового масиву;

– шифрування за один раунд усього блоку даних (байт-орієнтована структура);

– виконання криптографічних перетворень як над окремими байтами масиву, так і над його рядками та стовпчиками.

– загальні характеристики AES:

– зашифровує і розшифровує 128-бітові блоки даних;

– дає змогу використовувати три різні ключі довжиною 128, 192 або 256 біт (залежно від довжини ключа версії шифру позначають AES-128, AES-192 або AES-256);

– від розміру ключа залежить кількість раундів шифрування: довжина 128 біт – 10 раундів; довжина 192 біта – 12 раундів; довжина 256 біт – 14 раундів;

– усі раунди, крім останнього, ідентичні.

Для АПК можна обирати деякі симетричні алгоритми шифрування із вищенаведених, в залежності від степені конфіденційності інформації. Але необхідно враховувати, що недоліком симетричного шифрування є те, що секретний ключ повинен бути відомий як відправнику, так і одержувачу. З одного боку, це викликає нову проблему відправки ключів. З іншого боку, одержувач на підставі існування зашифрованого і розшифрованого повідомлення не може довести, що отримав повідомлення від конкретного відправника, оскільки міг згенерувати одне і те ж повідомлення.

ОСНОВНІ ПРАВИЛА ЩОДО КІБЕРБЕЗПЕКИ БУХГАЛТЕРСЬКИХ ДАНИХ НА ПІДПРИЄМСТВАХ

Поливана Л.А., канд. екон. наук, доц.
Луценко О.А., канд. екон. наук, доц.
Державний біотехнологічний університет

Цифрова трансформація змінила правила поведінки бухгалтерів у повсякденному їх житті. Кожне підприємство зіткнулося з реальним світом, в якому технологічний розвиток та поява нових кіберзагроз сунеться швидкими темпами. Зростаюча залежність від технологій та зберігання конфеденційних бухгалтерських даних в цифрових форматах роблять підприємства привабливими цілями для кіберзлочинців. Несанкціонований доступ до цієї інформації може мати серйозні наслідки, включаючи фінансові втрати. Підприємства, які не використовують в своїй дяльності кібербезпеку, зазнають нових вразливостей, які загрожують їх діяльності. Щоб орієнтуватися в цій складній ситуації, бухгалтери повинні збалансовувати використання технологій для зростання та інновацій, одночасно захищаючі свої системи та дані від загроз. В цю епоху бухгалтери повинні залишатися інформованими та приймати надійні міри кібербезпеки для захисту своїх цифрових активів.

Кібербезпеку даних в бухгалтерському обліку розглянуто в працях таких вчених, як Бутинець Ф.Ф., Євдокимов В.В., Івахненко С.В., Палій В.Ф., Пушкар М.С., Шквір В.Д. Однак проблеми кібербезпеки даних бухгалтерського обліку вирішені недостатньо. Саме відсутність глобального керування та введених в дію стандартів кібербезпеки полегшують кіберзлочинцям виявлення та здійснення хакерських атак, тому що кіберзагрози не сповільнилися, а навпаки стали ще більш складними та витонченими.

Законом України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. №2163-VIII визначаються правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у