УДК 636.4.082

ЗНАЧЕННЯ, БЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ У ТВАРИННИЦТВІ

Волощук В.М., доктор сільськогосподарських наук, член-кореспондент НААН
http://orcid.org/0000-0001-6980-1293
Підтереба М.О., аспірант*
Засуха Л.В., кандидат сільськогосподарських наук
Інститут свинарства і агропромислового виробництва НААН
вул.Шведська Могила, 1, м.Полтава, 36013, Україна
E-mail: pigbreeding@ukr.net

У наш час значення інформаційних ресурсів та шляхи безпечного збереження накоплених даних є основною проблемою функціонування будь-якої установи чи структурного підрозділу. Показано, що кожна структурна виробнича чи адміністративна одиниця має свої активи і у разі порушення їх системи захисту може спричинити вірогідні збитки через витік, спотворення, недоступність або видалення накопленої інформації.
При широкому впровадженні комп'ютерної техніки, коли більшість службової та особистої інформації переноситься з паперових носіїв на електронні, питання інформаційної безпеки службових та індивідуальних даних від несанкціонованого доступу набирає все більшого значення, а захищеною автоматизованою системою може бути лише та, яка має відповідні сучасні механізми захисту інформаційних ресурсів.
Дотримання основних правил захисту та конфіденційності, дозволить уникнути більшості можливих ризиків загрози цілісності інформаційних ресурсів.

Ключові слова: інформаційні ресурси, безпека даних, ризики пошкодження даних, забезпечення обмеженого доступу.

Розвиток галузі тваринництва на сучасному етапі технологічного прогресу змушує практично всі господарства відмовлятися від паперових носіїв і все більше переходити на електронні форми ведення обліку та передачі звітних даних.

Безперечно, такий підхід значно спрощує збір, накопичення, обробку та аналіз поточної виробничої інформації, але й несе у собі значний ризик втрати або пошкодження накопленої інформації. Ризики пошкодження зростають у зв'язку з необхідністю щоденно використовувати мережу інтернет, через яку до комп'ютера користувачів можуть потрапити шкідливі програми (комп'ютерні віруси) або за допомогою хакерських атак буде отримано доступ до накопичених даних.

З кожним роком ускладнюється система управління інформаційною сферою як у державі в цілому, так і окремих структурах виробничої та адміністративної діяльності, тому це підвищує рівень відповідальності кожного працівника, який має доступ до збору, накопичення, аналізу та використання накопленої інформації. В умовах постійного підвищення глобалізації суспільства, інформація стає стратегічним продуктом, а доступ до її носіїв – підвищує відповідальність за її збереження. Все більш широке запровадження нової комп'ютерної техніки та нового програмного забезпечення посилює необхідність захисту інформаційних ресурсів від впливу зовнішніх загроз, зокрема це стосується питань загального документообігу. Поява загроз втрати документів, в тому числі їх конфіденційності, обумовлена як внутрішніми, так і зо-

** Науковий керівник – доктор сільськогосподарських наук, професор, член-кореспондент НААН В.М. Волощук*

внішніми чинниками роботи сучасних інформаційно-комунікаційних систем. Недостатня захищеність інформаційних ресурсів може стати причиною порушення роботи інформаційного каналу та економічних збитків, внаслідок некоректного отримання, обробки та передачі даних. Розвиток засобів та механізмів збору, накопичення, зберігання, обробки та обміну інформацією є одними з найважливіших складових інтересів в інформаційній сфері будь-якої виробничої чи управлінської структури.

Для забезпечення інформаційної безпеки виробничих структур, необхідно насамперед вирішити завдання забезпечення конфіденційності, цілісності та доступності, що потребує створення відповідного інструментарію для їх здійснення.

Оскільки в даний час інформація вже стала товаром та потужним ресурсом впливу, необхідно щоб інформаційні ресурси, особливо, ті що містять конфіденційну, службову, виробничу або економічну інформацію, були надійно захищені від проникнення сторонніх осіб та вірусних атак.

Аналіз останніх досліджень і публікацій. Останнім часом все частіше піднімається питання захисту і збереження інформації та ефективного використання інформаційних ресурсів. Поняття «інформаційний ресурс» вперше було наведено у Законі України «Про Концепцію Національної програми інформатизації» – сукупність документів в інформаційних системах (бібліотеках, архівах, банках даних тощо). У концепції формування системи національних електронних інформаційних ресурсів визначено що національні електронні інформаційні ресурси – це ресурси незалежно від їх змісту, форми, години та місця створення, форми власності, призначені для задоволення потреб громадянина, суспільства, держави.

Поняття інформаційних ресурсів поділяють за основним змістом на правові, технічні, наукові, статистичні, фінансові, ЗМІ і т.д. Окремий поділ інформаційних ресурсів формується за ознакою власника (за правом власності), або за цілями: знання, ресурс управління, ресурс виробництва й т.п. [1, 2, 3, 6]. У сучасній українській науковій літературі «інформаційні ресурси» визначають як сукупність інформації, зафіксованої на матеріальних носіях. Офіційне визначення інформаційних ресурсів, відповідно до наукового та загальновизнаного уявлення про них, пов'язують з поняттями документа [7, 13, 14].

Щоб будь-яка інформація стала інформаційним ресурсом який необхідно захищати, вона повинна мати соціальну значимість та технологічну цінність для її практичного використання. Входження у глобальний інформаційний простір дозволяє функціонувати й розвиватись міжнародним відносинам, зокрема економічним, політичним, соціальним та культурним процесам, що дозволяє створювати принципово нові умови функціонування, розвитку й використання інформаційних ресурсів. Отже активний розвиток інформаційної сфери та застосування сучасних інформаційних технологій, суттєво впливає на процеси розвитку суспільства і стає головною складовою використання у різних сферах виробничої діяльності та визначає необхідність захисту від несанкціонованого втручання у її роботу [5, 8, 9, 10].

Таким чином постає питання конфіденційності даних, які представляють собою особливу цінність. Важливе значення мають виробничі показники у сільському господарстві, серед яких можна виділити: технологічні, зоологічні, генетичні, годівельні, селекційні та інші показники, які необхідно зберегти, дотримавши їх конфіденційність. Зокрема, навіть якщо допустити, що приведені вище показники можуть досі утримуватись на паперових носіях, то всі показники отримані з електронно-обчислювальних апаратів, в першопочатковому виді будуть отримані виключно з електронних носіїв, на яких в подальшому будуть і зберігатись. Серед таких даних можна виділити такі як:

– Інформація із спутників GPS, що отримують дані про точне місцезнаходження датчиків, які можуть бути прикріплені на сільськогосподарські об'єкти, в тому числі на сільськогосподарську техніку чи тварин.

- Дані електронних карт, які дозволяють отримувати, аналізувати та обробляти зображення для створення просторової інформації, яка необхідна для визначення стану господарства, в тому числі його змін.
- Дані отримані з електронно-вимірювальних апаратів, що дозволяють робити заміри технологічних, біологічних чи екологічних показників.
- Дані дистанційних датчиків, які функціонують за принципом дистанційного визначення стану ґрунтів, рослин, наявності шкідників та ін.
- Дані бортових датчиків, які застосовуються для визначення стану врожаю, наявності та кількості добрив, вологості ґрунту, хімікатів та ін.

Розвинуті країни світу (Німеччина, Данія, Велика Британія, США, Японія, Китай) використовують інформаційні технології з 80-х років минулого століття та отримують від цього значну перевагу на внутрішньому та зовнішньому ринку.

Інформаційні технології можуть допомагати не лише підтримувати вчасне інформування про стан поточного господарства, але і здійснювати управління господарством в цілому, тому дуже важливим аспектом є захист таких даних, їх збереження та конфіденційність.

Мета і завдання. Основною метою даної роботи є розкриття важливості інформаційних ресурсів, оцінки їх застосування та збереження від несанкціонованого копіювання, блокування чи знищення.

Результати досліджень та їх обговорення. Кожна структурна виробнича чи адміністративна одиниця має свої активи, тобто все те що є цінним і залежить від важливості для ефективної діяльності установи чи організації [4, 5]. Зокрема коли мова йде про безпеку системи інформаційних ресурсів, які використовуються у певній організації, то при її оцінці звертають увагу на питання вірогідних збитків через витік, спотворення, недоступність та/або руйнування баз даних або іншої інформації. Таким чином безпека інформаційних ресурсів – це комплексна система заходів яка передбачає загальну захищеність всіх видів інформації від несанкціонованого доступу: ознайомлення, оприлюднення, використання, внесення змін чи пошкодження, а також збереження повної конфіденційності, доступності і цілісності інформації.

Поняття «інформаційна безпека» виникло разом з появою засобів обміну інформацією між людьми, а також з усвідомленням наявності у осіб і установ інтересів завдання шкоди, шляхом впливу на засоби накопичення та передачі інформації. Захист інформації не обмежується безпекою технічних інформаційних систем у якій вона перебуває, в наслідок додаткових факторів ризиків втрати інформації.

При широкому впровадженні комп'ютерної техніки, питання інформаційної безпеки службових та індивідуальних даних почали вирішувати методами і засобами широкого обмеження фізичного доступу до обладнання, яке здійснює збір, занесення, аналіз і передачу інформації. При створенні і широкому запровадженні інформаційно-комунікаційних мереж, завдання інформаційної безпеки вирішуються методами не лише обмеження фізичного доступу до пристроїв, об'єднаних у локальну мережу чи мережу інтернет, а й шляхом введення обмеженого доступу до ресурсів, як введення права лише на перегляд, без права внесення змін, копіювання та передачі (надсилання) даних третім особам. Ці права надаються лише співробітникам з правом адміністративного доступу.

З появою безпровідних систем прийому та передачі інформації, було розроблено нові критерії безпеки, які включали нові протоколи захисту, та способи багатофакторної автентифікації.

Захищеною автоматизованою системою може бути лише та, яка має наявні відповідні сучасні механізми захисту інформаційних ресурсів, тобто коли всі шляхи реалізації виявлених загроз будуть перекриті механізмами захисту, які відповідають рівню

можливих ризиків та співвідносяться як за вартістю витрат на їх реалізацію, так і за вартістю очікуваних фінансових втрат від несанкціонованого проникнення у інформаційну мережу. Побудова оптимальних систем захисту потребує урахування великого числа параметрів які необхідно оцінити та запобігти їх пошкодженню.

Склад активів які підлягають захисту це комп'ютерне обладнання та програмне забезпечення різного призначення, а також нематеріальні активи, як то репутація, імідж організації, рівень її ділової активності, перелік робіт, замовлень від організацій-суміжників, постачальників, списки продукції яка виробляється і постачається організацією, та інше.

Для встановлення критеріїв та рівня необхідної інформаційної безпеки необхідно визначитись:

- наскільки важливо захистити дану частину інформаційної діяльності, тобто наскільки вона повинна бути закритою;
- які профільні (виробничі) задачі організації можуть бути реалізовані тільки за допомогою інформаційних технологій.
- яка група даних потребує захисту і яку шкоду підприємству може нанести її витік або пошкодження.
- яке програмне забезпечення та яку технічну підтримку буде використовувати організація.

Для встановлення цінності активів які повинні підлягати захисту, потрібно приймати до уваги:

1. вартість створення та обслуговування активу;
2. вартість модернізації та відновлення активу;
3. збиток що наноситься організації у випадку порушення конфіденційності, цілісності або доступності інформаційних активів;
4. комбінація трьох попередніх варіантів, дає змогу отримати певну інтегральну оцінку загальної цінності активу.

Наступним кроком при визначенні інформаційного захисту повинно бути визначення степені впливу на:

- зниження рівня ділової активності організації;
- втрати/погіршення репутації організації;
- фінансових втрат;
- перебоїв у виконанні ділових операцій;
- погіршенню інвестиційного клімату;

Інформаційні системи маючи уразливість можуть піддаватись атакам та пошкоджуватись, що є причиною матеріальних та нематеріальних збитків. Уразливість – це комплекс недоліків при проектуванні та написанні програмного забезпечення, зумовлений особливостями виконання програмного коду під тією чи іншою операційною системою, що призводить до порушення безпеки конкретного мережевого чи індивідуального ресурсу. Атака – це фізична реалізація загрози, яка проявляється або у спробі проникнення в інформаційну мережу, у несанкціонованому втручанні у її роботу, або копіювання чи пошкодження конфіденційності даних. Внаслідок таких втручань установа або особа може нести збитки, які виражаються у втраті майна, фінансів чи нанесенні моральної шкоди та шкоди іміджу і діловим партнерським відносинам, втраті замовників, розриву контрактів, зменшення товарного та інформаційного обігу [11, 12].

Щоб уникнути несанкціонованого проникнення та успішної реалізації інформаційних атак які можуть нести загрозу конфіденційності, доступності, цілісності, модифікації (спотворення), копіювання, втрати, блокування або знищення інформації, необхідно максимально обмежити мережу (персональний комп'ютер) від вільного до-

ступу до мережі інтернет, шляхом створення локальної мережі яка не має прямого виходу на сервери інтернету, а вихід на зовнішнє інформаційне поле здійснюється лише через комп'ютер адміністратора. У всіх інших випадках на кожному комп'ютері має бути система антивірусного захисту з постійним оновленням антивірусної бази даних.

Висновок: Загроза цілісності інформаційних ресурсів може бути різносторонньою і непередбачуваною, але за допомогою дотримання основних правил захисту, збереження та конфіденційності можна уникнути більшості можливих ризиків. Головним у знешкодженні вірогідних загроз є дотримання правил безпеки при користуванні комп'ютером, в тому числі виходом в інтернет.

БІБЛІОГРАФІЯ

1. Барсуков, В.С. 2001. Безпека: технології, засоби, послуги. М., 496.

2. Барсуков, В.С., та В.В. Водолазський. 2000. Сучасні технології безпеки. М.: Нолидж, 496.

3. Бачило, И.Л., В.Н. Лопатин, та М.А. Федотов. 2005. Информационное право: Учебник. СПб., 725.

4. Закон України «Про Концепцію Національної програми інформатизації від 4 лютого 1998 року №75/98–ВР. //Відомості Верховної Ради України. 1998. № 27–28.

5. Зегжда, Д.П. 2000. Основи безпеки інформаційних систем. 2009. / Д.П. Зегжда, А.М. Івашко. – М.: Гаряча лінія – Телеком, 452 с., Мул 1. Казакова Н. Ф. Принципи побудови захищених інтелектуальних мереж. / Н. Ф. Казакова // *Вісник ДУІКТ. – К. : ДУІКТ.* 2009. № 4. 381–388.

6. Інформаційна безпека людини як споживача телекомунікаційних послуг : Монографія / І.В. Арістова, Д.В. Сулацький ; НДІ інформатики і права НАПрН України. – К. : Право України; Х. : Право, 2013. 184.

7. Казакова, Н. Ф. 2010. Доповнення до концепції інформаційної безпеки Сучасна спеціальна техніка. К.: Державний НДІ МВС України. № 3(22). 74–80.

8. Казакова, Н. Ф. 2009. Системний аналіз особливостей впровадження захищених інформаційних мереж в Україні та синтез критерію їх ефективності / О. О. Скопа, Н. Ф. Казакова. Наукові записки Міжнародного гуманітарного університету. О.: МГУ. № 16. 115–122.

9. Казакова, Н. Ф. 2010. Аналіз напрямів розвитку інформаційної безпеки у комп'ютерних системах та мережах на основі застосування програмних засобів захисту інформації. *Вісник Львівського національного аграрного університету.* Л.: Львівський нац. агроун-т. № 14. 47–57.

10. Казакова, Н. Ф. 2009 Наукові задачі синтезу організаційно-технологічної схеми створення програмного забезпечення для комп'ютерних мереж з обмеженим доступом / В. О. Хорошко, Н. Ф. Казакова // Захист інформації. К. : ДУІКТ. № 4(45). 11 – 18.

11. Леонов, А.П. 2000. Комп'ютерна злочинність та інформаційна безпека. Мінськ: арил. 552.

12. Кормич, Б. А. 2004. Інформаційна безпека: організаційно-правові основи: Навч. посібник. К.: Кондор, 384.

13. Цимбалюк, В.С. 2001. Проблеми державної інформаційної політики: гармонізація міжнародного і національного інформаційного права. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. К.: НТУУ «КПІ». № 4.

14. Ярочкін, В.І. 2005. Інформаційна безпека. Підручник для студентів вузів. 3-е вид. – М.: Академічний проект: Трікста, 544.

REFERENCES

1. Barsukov, V.S. 2001. Bezpeka: tekhnolohii, zasoby, posluhy – Security: technologies, tools, services. – M., 496 (in Ukrainian).

2. Barsukov, V.S., Vodolazskyi, V.V. 2000. Suchasni tekhnolohii bezpeky – Modern security technologies – M.: Nolidzh. 496, IL. (in Ukrainian).

3. Bachylo, L.L., Lopatin, V.N., Fedotov, M.A. 2005. Information Law: Textbook. – SPb. 725 (in Ukrainian).

4. Zakon Ukrayiny «Pro Kontseptsiyu Natsionalnoi prohramy informatyzatsii vid 4 liutoho 1998 roku №75/98–VR. – //Vidomosti Verkhovnoyi Rady Ukrayiny. – 1998. Law of Ukraine "On the Concept of the National Program of Informatization of February 4, 1998 No. 75/98-VR. – // The Bulletin of the Verkhovna Rada of Ukraine, 27-28 (in Ukrainian).

5. Zehzhda, D.P., Ivashko, A.M. 2009. Osnovy bezpeky informatsiinykh system: Haryacha liniya – Telekom, , Mul 1. Kazakova, N. F. Pryntsypy pobudovy zakhyshchenykh intelektual-nykh merezh [Tekst]. Visnyk DUIKT. – K. : DUIKT, 4: 381–388. Basics of security of information systems: Hotline – Telecom, 452, Muli 1. Kazakova, N.F. Principles of construction of protected intellectual networks [Text]. Visinyk DUIKT. – K.: DUIKT, 4: 381-388 (in Ukrainian).

6. Aristova, I.V. Sulatskyi, D.V. 2013. Informatsiyna bezpeka lyudyny yak spozhyvacha telekomunikatsiynykh posluh: Monohrafiia. NDI informatyky i prava NAPrN Ukrayiny. – Information security of a person as a consumer of telecommunication services: Monograph :Research Institute of Informatics and Law of the National Academy of Sciences of Ukraine. – K.: K. : Pravo Ukrayiny; KX. : Pravo, 184 (in Ukrainian).

7. Kazakova, N.F. 2010. Dopovnennya do kontseptsiyi informatsiynoyi bezpeky [Tekst]. Suchasna spetsialna tekhnika. –Addendum to the concept of information security [Text]. Modern Special Technique. – K. : Derzhavnyy NDI MVS Ukrayiny. 3 (22): 74-80 (in Ukrainian).

8. Kazakova, NF., Skopa, O.O. 2009. Systemnyy analiz osoblyvostey vprovadzhennya zakhyshchenykh informatsiynykh merezh v Ukrayini ta syntez kryteriyu yikh efektyvnosti [Tekst]. Naukovi zapysky Mizhnarodnoho humanitarnoho universytetu. –System analysis of the peculiarities of the implementation of secure information networks in Ukraine and synthesis of the criterion of their effectiveness [Text] Scientific notes of the International Humanitarian University. – O.: MSU, 16: 115-122 (in Ukrainian).

9. Kazakova, N.F. 2010. Analiz napryamiv rozvytku informatsiynoi bezpeky u kompiuternykh systemakh ta merezhakh na osnovi zastosuvannia prohramnykh zasobiv zakhystu informatsii [Tekst]. Visnyk Lvivskoho natsionalnoho ahrarnoho universytetu. – L. : Lvivskyy nats. ahroun-t. –An analysis of the directions of development of information security in computer systems and networks on the basis of application of software for information security [Text]. Visnyk Lvivskoho natsionalnoho ahrarnoho universytetu. – L. : Lvivskyy nats. ahroun-t., 14: 47-57 (in Ukrainian).

10. Kazakova, N.F., Khoroshko, V.O. 2009. Naukovi zadachi syntezu orhanizatsiyno-tekhnolohichnoyi skhemy stvorennya prohramnoho zabezpechennya dlya kompyuternykh merezh z obmezhenym dostupom [Tekst]. Zakhyst informatsiyi. –Scientific tasks of synthesis of organizational and technological scheme of software development for computer networks with restricted access [Text]. Information protection. – K.: DUIKT, 4 (45): 11 – 18.

11. Leonov, A.P. 2000. Komp'yuterna zlochynnist ta informatsiyna bezpeka. – Computer Crime and Information Security. – Minsk: aryl, 552 (in Ukranian).

12. Kormych, B.A. 2004. Informatsiyna bezpeka: orhanizatsiyno-pravovi osnovy: Navch. posibnyk. –Information Security: Organizational and Legal Foundations: Teaching. manual. – K.: Kondor, 384 (in Ukrainian).

13. Tsymbaliuk, B.C. 2001. Problemy derzhavnoyi informatsiynoyi polityky: harmonizatsiya mizhnarodnoho i natsionalnoho informatsiynoho prava // Pravove,

normatyvne ta metrolohichne zabezpechennya systemy zakhystu informatsiyi v Ukrayini. –Problems of State Information Policy: Harmonization of International and National Information Law // Legal, normative and metrological provision of the information security system in Ukraine. – K .: NTUU "KPI", 4 (in Ukraine).

14. Yarochkin, V.I. 2005. Informatsiyna bezpeka. Pidruchnyk dlya studentiv vuziv / 3-e vyd. – Informational security. Textbook for college students / 3rd form. – M .: Akademichnyy proekt: Triksta, 544 (in Ukrainian).

Волощук В.М., Подтереба М.А., Засуха Л.В. Значение, безопасность и защита информационных ресурсов в животноводстве

В наше время значение информационных ресурсов и пути безопасного хранения накопленных данных является основной проблемой функционирования любого учреждения или структурного подразделения. Показано, что каждая структурная производственная или административная единица имеет свои активы и в случае нарушения системы защиты которых может повлечь вероятные убытки из-за утечки, искажения, недоступность и удаления накопленной информации.

При широком внедрении компьютерной техники, когда большинство служебной и личной информации переносится с бумажных носителей на электронные, вопросы информационной безопасности служебных и личных данных от несанкционированного доступа набирает все большее значение, а защищенной автоматизированной системой может быть только та, которая имеет соответствующие современные механизмы защиты информационных ресурсов.

Соблюдение основных правил защиты и конфиденциальности позволит избежать большинства возможных рисков угрозы целостности информационных ресурсов.

Ключевые слова: информационные ресурсы, безопасность данных, риски повреждения данных, обеспечение ограниченного доступа.

Voloshchuk V.M., Pidtereba M.O., Zasukha L.V. Importance, security and protection of information resources in livestock-breeding

Nowadays, the importance of information resources and the ways to safely store the accumulated data is the main problem of the functioning of any institution or structural unit. It is shown that each structural production unit or administrative unit has its assets and, in case of violation of their system of protection, may cause probable losses due to leakage, distortion, inaccessibility and / or deletion of accumulated information.

With the widespread introduction of computer technology, when most of the official and personal information is transferred from paper media to electronic, the issue of information security of service and personal data from unauthorized access is gaining the increasing importance, and the protected automated system can only be that which has appropriate modern mechanisms of protection of information resources.

Following the basic rules of protection and confidentiality will allow to avoid the majority of possible risks for the integrity of information resources.

Key words: information resources, data security, data corruption risks, provision of restricted access.