

УДК 65.012.8

ВАЖЛИВІСТЬ ЗАХИСТУ ІНФОРМАЦІЇ СІЛЬСЬКОГОСПОДАРСЬКИХ
ПІДПРИЄМСТВ

THE IMPORTANCE OF DATA PROTECTION FOR AGRICULTURAL
ENTERPRISES

*РОМАНАШЕНКО М.О., РОМАНАШЕНКО І.О.,**

здобувачки другого (магістерського) рівня вищої освіти
Харківський національний технічний університет сільського
господарства імені Петра Василенка

В роботі розкрито сутність понять загроза безпеки інформації та захист інформаційної системи на сільськогосподарських підприємствах. Розглянуто та проаналізовано елементи інформаційної безпеки, адже від їх стану на пряму залежить рівень захисту інформаційних даних у процесі сільськогосподарських відносин та ведення господарської діяльності. Наведено необхідність проведення заходів для захисту даних та розглянуто основні причини порушення конфіденційності інформації на сільськогосподарських підприємствах.

***Ключові слова:** інформаційна безпека, захист інформації, загроза безпеки, викрадення даних, діджиталізація.*

Essence of concepts is in-process exposed threat of safety of information and defense of the informative system on agricultural enterprises. The elements of informative safety are considered and analyzed, in fact from their state straight the level of protection of informative data depends in the process of agricultural relations and conduct of economic activity. A necessity over of realization of events is brought for the protection of data and principal reasons of violation of confidentiality of information are considered on agricultural enterprises.

***Keywords:** informative safety, defense of information, threat of safety, theft of data, digitalization.*

Постановка проблеми у загальному вигляді. В період глобалізаційних перетворень інформаційного простору та технологічної інформатизації усіх сфер життя суспільства гостро стоїть проблема захисту інформації від загроз та некоректного втручання у кібернетичному просторі та визначення економічної доцільності організації захисту інформації на сільськогосподарських підприємствах.

Аналіз останніх досліджень і публікацій. Через актуальність теми та широкий резонанс велика кількість сучасних науковців приділяють увагу вивченню інформаційної безпеки на підприємствах світу в цілому та України зокрема. На дослідження проблем інформаційної безпеки у секторі сільського господарства звертали свою увагу такі науковці як: Ткачук В.І. [9], Яремова М.І. [9], Ортинський В.Л. [7], Живко З.Б. [7], Кавун С.В. [5], Пилипенко А.А. [5] та ін.

Формулювання цілей статті. Метою статті є дослідження сучасних загроз для інформації підприємств сільського господарства з боку кіберпростору.

Виклад основного матеріалу дослідження. Можливості кібернетичного простору, швидкі темпи розвитку та впровадження новітніх інформаційних технологій забезпечують умови для накопичення та використання інформації, а також створюють основоположну залежність від їх нормального функціонування всіх сфер життєдіяльності суспільства та держави: економіки, політики, сфери національної та міжнародної безпеки тощо. Така залежність стає вразливим місцем у функціонуванні систем та об'єктів національних інфраструктур і дає можливість негативно налаштованим елементам та угрупованням скористатися нею для реалізації протиправних дій у кібернетичному просторі шляхом порушення цілісності, доступності, конфіденційності інформації та нанесення шкоди інформаційним ресурсам і системам [1, с. 59].

* Науковий керівник: к.е.н., доцент Поливана Л.А

Важливість формування захисту потоку інформаційних даних – це не нова потреба у процесі глобалізації та діджиталізації сільськогосподарських підприємств. Але, зважаючи на неупинний розвиток хакерських програм та способів викрадення і зараження даних на тлі кволих темпів розвитку сфери захисту інформації, з кожним роком це питання стає більш гострим, а пошук шляхів розв'язання – нагальнішим. Керівники середніх і великих аграрних компаній вже усвідомлюють наявність усіх ризиків, пов'язаних з інформаційною складовою, тому підтримку високого рівня інформаційної безпеки відносять до пріоритетних завдань.

Під загрозою безпеки інформації розуміються сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері [6].

До об'єктів інформаційної безпеки сільськогосподарських підприємств відносять: — інформаційні ресурси, що містять відомості, віднесені до комерційної таємниці, та конфіденційну інформацію, представлену у вигляді інформаційних масивів і баз даних; — засоби і системи інформатизації — засоби обчислювальної та організаційної техніки, мережі та системи, загальносистемне і прикладне програмне забезпечення, автоматизовані системи управління в організаціях, системи зв'язку і передачі даних, технічні засоби збору, реєстрації, передачі, обробки та відображення інформації [9].

Значна загроза найчастіше є наслідком помилок в програмному забезпеченні автоматизованої інформаційної системи. Також не варто забувати, що основними причинами пошкодження, викрадення та некоректного відображення даних можуть бути недостатній рівень володіння знаннями у сфері захисту конфіденційної інформації, застосування не ліцензійних та не сертифікованих продуктів програмного забезпечення, недостатній контроль керівників структурних підрозділів за дотриманням усіма працівниками правил захисту інформації, думка, що забезпечення інформаційної безпеки сільськогосподарського підприємства – це одноразовий акт.

Метою кібератаки можуть бути вимагання грошей та шантаж, популяризація шахрая, який здійснює напад, дестабілізація ситуації.

Зловмисники можуть використовувати різні методи для несанкціонованого збору даних. Зокрема доступ до баз даних, прослуховування каналів, під'єднання до локальної мережі підприємства тощо. Система захисту інформації як організована сукупність органів спеціального призначення на сільськогосподарських підприємствах повинна відповідати певним вимогам (рис. 1).

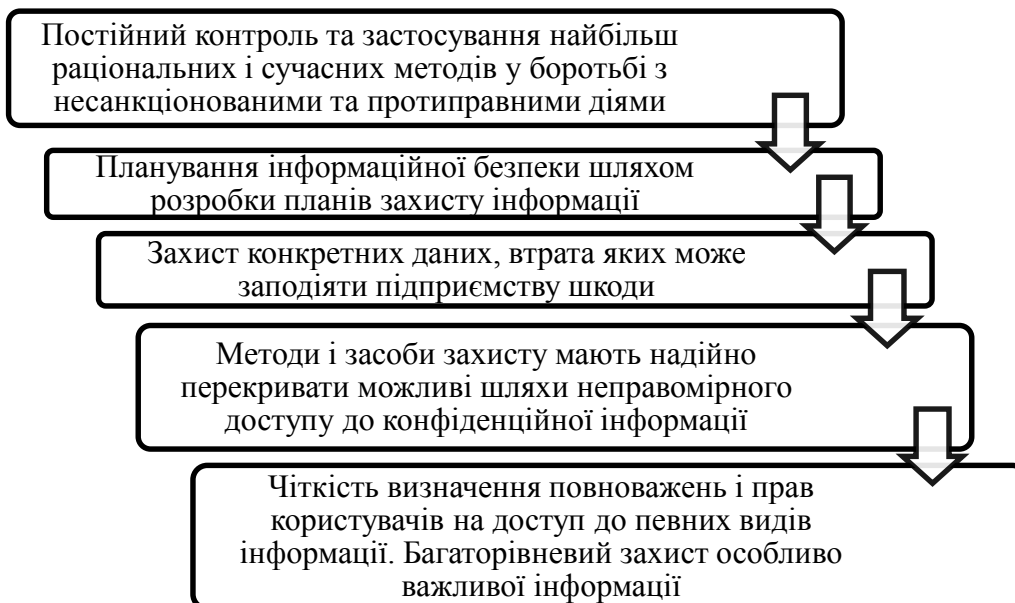


Рис. 1. Основні вимоги до системи захисту інформації
Джерело: складено автором

Суттєве зрушення, яке відбулося у сфері української кібербезпеки – законодавче врегулювання. 16 лютого 2017 року було ухвалено рішення від 29.12.2016 року Радою національної безпеки і оборони України «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» №п0015525-16, за поточною редакцією від 16.02.2017 року [8]. 21 червня 2018 року набув чинності Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII, поточна редакція від 03.07.2020 року [3].

Відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» № 80/94-ВР, захист інформації в системі — діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі [4].

Для захисту інформації потрібна не просто розробка приватних механізмів захисту, а реалізація системного підходу, що містить комплекс їх взаємозв'язку. Головною метою будь-якої системи забезпечення інформаційної безпеки є створення умов функціонування підприємства, запобігання кіберзагроз його безпеки, захист законних інтересів підприємства від протиправних посягань, недопущення розкрадання фінансових засобів, розголошення, втрати, витоку, спотворення і знищення службової інформації, забезпечення в рамках діяльності установи [2, с. 157].

Висновки. Отже, важливість захисту даних в умовах загальнодоступності більшої частки інформації важко переоцінити. Керівники усіх організаційних рівнів сільськогосподарського підприємства мають усвідомлювати наслідки кібератаки та витоку конфіденційної інформації. Необхідність застосування систем захисту на сільськогосподарських підприємствах зумовлена також високою привабливістю сектору для інвесторів та інноваторів. Тому наявність надійного та ліцензованого захисного бар'єру створить більш сприятливі умови для інвестування в агропромисловий сектор економіки України.

Література.

1. Бурячок В.А., Толюпа С.В., Семко В.В. Інформаційний та кіберпростори. Проблеми безпеки, методи та засоби боротьби. Навч. посіб. Київ: Наш формат, 2016. 176с.
2. Бурячок В.А., Толюпа С.В., Толубко В.Б., Хорошко В.О. Інформаційна та кібербезпека: соціотехнічний аспект. Навч. посіб. Київ: Наш формат. 2015. 288с.
3. Закон України «Про основні засади забезпечення кібербезпеки України» №2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 19.04.2021р.).
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» №80/94-ВР. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text> (дата звернення: 19.04.2021р.).
5. Кавун С.В., Пилипенко А.А., Ріпка Д.О. Економічна та інформаційна безпека підприємств у системі консолідованої інформації. Навчальний посібник. Харків: ХНЕУ. 2013. 362с.
6. Класифікація загроз в інформаційній безпеці. URL: <https://sites.google.com/site/infobezosob/klasifikacia-zagroz-informacijnij-bezpeci> (дата звернення: 11.04.2021р.).
7. Ортинський В.А., Керницький І.С., Живко З.Б. Економічна безпека підприємств. Підручник. Київ: Алерта. 2011. 702с.
8. Рішення Ради національної безпеки і оборони України «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» від 29.12.2016 року №п0015525-16. URL: <https://zakon.rada.gov.ua/laws/show/n0015525-16#Text> (дата звернення: 26.04.2021р.).
9. Ткачук В.І., Яремова М.І. Економічна безпека сільськогосподарських підприємств. *Ефективна економіка*. 2019. №6. URL: <http://www.economy.nayka.com.ua/?op=1&z=7100> (дата звернення: 15.04.2021р.).
10. Securityforum ISF 2021. «Threat Horizon 2023: Security at a tipping point». URL: <https://www.securityforum.org/research/threat-horizon-2023-security-at-a-tipping-point/>. (дата звернення: 15.04.2021р.).



References

1. Burjachok V., Toljupa S. and Semko V., 2016. Informacijnyj ta kiberprostory. Problemy bezpeky, metody ta zasoby borotjby. Kyjiv: Nashformat, p.176.
2. Burjachok V., Toljupa S., Tolubko V. and Khoroshko V., 2015. Informacijna ta kiberbezpeka: sociotekhnichnyj aspekt. Kyjiv: Nash format, p.288.
3. Zakon Ukrainy «Pro osnovni zasady zabezpechennja kiberbezpeky Ukrainy» [The Law of Ukraine «On the basic principles of cyber security in Ukraine»] Retrieved from <https://zakon.rada.gov.ua/laws/show/80/94-D0%B2%D1%80#Text> (accessed 19 April 2021).
4. Zakon Ukrainy «Pro zakhyst informacii v informacijno-telekomunikacijnykh systemakh» [The Law of Ukraine «On Protection of Information in Automated Systems»] Retrieved from <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text> (accessed 19 April 2021).
5. Kavun S., Pylypenko A. and Ripka D., 2013. Ekonomichna ta informacijna bezpeka pidprijemstv u systemi konsolidovanoji informacii. Kharkiv: KhNEU, p.362.
6. Klasyfikacija zagroz informacijnij bezpeci. [online] Retrieved from <https://sites.google.com/site/infobezosob/klasifikacia-zagroz-informacijnij-bezpeci> (accessed 11 April 2021).
7. Ortyns'kyj V., Kernyc'kyj I. and Zhyvko Z., 2011. Ekonomichna bezpeka pidprijemstv. Kyjiv: Alerta, p.702.
8. Rishennja Rady nacional'noji bezpeky i oborony Ukrainy «Pro zagrozy kiber bezpeci derzhavy ta nevidkladni zakhody z jikh nejtralizacii» [Decision of the National Security and Defense Council of Ukraine «On threats to cybersecurity of the state and urgent measures to neutralize them»] vid 29.12.2016 roku №n0015525-16. Retrieved from <https://zakon.rada.gov.ua/laws/show/n0015525-16#Text> (accessed 26 April 2021).
9. Tkachuk V. and Jareмова M., 2019. Ekonomichna bezpeka sil's'koghospodars'kykh pidprijemstv. Efektyvna ekonomika, [online] (6). Retrieved from <http://www.economy.nayka.com.ua/?op=1&z=7100> (accessed 15 April 2021).
10. Securityforum ISF 2021. «Threat Horizon 2023: Security at a tipping point». Retrieved from <https://www.securityforum.org/research/threat-horizon-2023-security-at-a-tipping-point/>. (accessed 15 April 2021).

