УДК 658.3: 007: 631.15
DOI: https://doi.org/10.36887/2415-8453-2019-4-8

Дмитро Володимирович ДЯЧКОВ

кандидат економічних наук, доцент,
доцент кафедри менеджменту, Полтавська державна аграрна академія
ORCID ID: 0000-0002-2637-0099
E-mail: dmiraf@ukr.net

СТРАТЕГІЧНІ НАПРЯМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ АГРОПРОДОВОЛЬЧОЇ СФЕРИ

Дячков, Д. В. Стратегічні напрями управління інформаційною безпекою підприємств агропродовольчої сфери [Текст] / Дмитро Володимирович Дячков // Український журнал прикладної економіки. – 2019. – Том 4. – № 4. – С. 70–78. – ISSN 2415-8453.

Анотація

Метою *статті є дослідження стратегічних напрямів управління інформаційною безпекою аграрних підприємств.*

Методи дослідження. *Вирішення поставлених у статті завдань здійснено за допомогою методів систематизації та узагальнення, аналізу та синтезу, діалектичного підходу.*

Результати дослідження. *В процесі дослідження визначено основні елементи формування та реалізації інформаційної стратегії аграрних утворень. Охарактеризовані зацікавлені сторони у формуванні та реалізації стратегії інформаційної безпеки аграрного підприємства. Надано характеристику основних дев'яти типів інформаційних стратегій: профілактична стратегія, стратегія стримування, стратегія спостереження, стратегія виявлення, стратегія реагування, стратегія відволікання, стратегія захисту по периметру, стратегія компартменталізації, стратегія шарування. На основі узагальнення стратегій інформаційної безпеки підприємств агропродовольчої сфери визначено ключові напрями її формування та реалізації.*

Побудовано логіко-структурну схему процесу формування стратегії захисту інформації, який повинен перебувати у тісному взаємозв'язку з основними бізнес-цілями підприємства та його загальною стратегією. Розглянуто актуальні тенденції та кращі практики розвитку інформаційної безпеки підприємства.

Висновки. *Проведене дослідження дало змогу визначити сутність інформаційної стратегії аграрних підприємств як структурованому і взаємопов'язаному набору виважених дій, спрямованих на довгострокову перспективу захисту інформаційних об'єктів підприємства.*

Практичне значення. *Запропонований процес формування інформаційної стратегії аграрних утворень дозволить аграрним підприємствам обрати оптимальну інформаційну стратегію, яка буде взаємообумовленою із загальною стратегією розвитку та дозволить сформувати необхідний набір програмних, технічних, апаратних та організаційних інструментів захисту інформаційних ресурсів.*

Перспективи подальших досліджень *передбачають розробку методології визначення стратегії інформаційної безпеки аграрного підприємства.*

Ключові слова: *аграрне підприємство, агропродовольча сфера, елемент, інформаційна безпека, стратегічний напрям, стратегія інформаційної безпеки, цифровізація.*

Dmytro DIACHKOV

Candidate of Economics (PhD), associate professor of
of the Department of Management, Poltava State Agrarian Academy

STRATEGIC DIRECTIONS OF INFORMATION SECURITY MANAGEMENT OF AGRO-FOOD ENTERPRISES

Abstract

The purpose *of the article was to study the strategic directions of information security management of agricultural enterprises.*

Research methods*. The tasks set out in the article were implemented using the methods of systematization and generalization, analysis and synthesis, dialectical approach.*

The results of the study*. In the research course the main elements of the formation and implementation of the information strategy of agrarian entities were identified. Stakeholders in the formation and implementation of the information security strategy of the agricultural enterprise were identified. The main nine types of information strategies were described. There are: prevention strategy, containment strategy, surveillance strategy, detection strategy, response strategy, distraction strategy, perimeter protection strategy, compartmentalization strategy, layering strategy. On the basis of generalization of information security strategies of the agro-food enterprises the key directions of its formation and realization were determined. A logical outline of the forming process an information security strategy was constructed, which should be closely related to the main business goals of the enterprise and its corporate strategy. The current trends and best practices of information security development of the enterprise were considered.*

Conclusions. *The research made it possible to determine the essence of information strategy of agricultural enterprises as a structured and interconnected set of weighted actions aimed at long-term protection of enterprise information objects.*

Practical value*. The proposed process of forming the information strategy of agricultural education will allow agricultural enterprises to choose the optimal information strategy, which will be interdependent with the general strategy and will allow to form the necessary set of software, technical, hardware and organizational tools for the protection of information resources.*

Prospects for further research *include the development of a methodology for determining the information security strategy of agrarian enterprise.*

Keywords*: agricultural enterprise, agro-food sector, element, information security, strategic direction, information security strategy, digitalization.*

JEL classification: M15; F52

Вступ

Сучасне агарне підприємство не може існувати без чітко сформованої та деталізованої стратегії. Основне завдання розробки стратегії полягає в пошуку шляхів подолання конкуренції на ринку, забезпеченні високих темпів економічного розвитку підприємства. Водночас, розвиток інформаційних технологій та пов'язаний з ним процес цифровізації, відкриває для сучасних підприємств значні можливості оптимізації бізнесу, підвищення конкурентоспроможності, ефективності та швидкості прийняття управлінських рішень тощо. Проте, є й інша сторона медалі, коли з новими можливостями з'являються і нові, не повністю вивчені ризики, пов'язані з інформаційною безпекою. Тому, забезпечення інформаційної безпеки аграрних підприємств в умовах швидкої зміни факторів зовнішнього середовища є важливою передумовою їх ефективного функціонування, а процес формування стратегії бізнесу суб'єктів агропродовольчої сфери обґрунтовує необхідність інтеграції стратегії їх інформаційної безпеки.

Варто відзначити, що окремі аспекти стратегічних напрямів захисту інформації та інформаційної стратегії розглянуто у працях Андерсона Е., Атіфа А., Бірюкова В., Вільямсона М., Євсеєва С., Кларка Дж., Левкова Я., Лихарева Н., Мейнарда С., Парка С., Перуна Т., Тапаіадора Дж., Чаплигіна Р., Чередниченко А., Чобінеха Дж.

Проте, особливості формування та реалізації інформаційної стратегії підприємства, зокрема підприємств агропродовольчої сфери, їх типізація, взаємообумовленість загальною стратегію у працях зарубіжних та вітчизняних вчених розглянута фрагментарно, що і визначає мету дослідження та підтверджує актуальність.

Мета дослідження

Формулювання цілей статті – дослідження стратегічних напрямів управління інформаційною безпекою аграрних підприємств.

Виклад основного матеріалу дослідження

Інформаційна архітектура сучасного аграрного підприємства, яка пронизує його виробничі та управлінські процеси потребує надійного та своєчасного захисту. Зазначене обґрунтовує необхідність формування політики захисту інформації та розробки й реалізації ефективної інформаційної стратегії, яка повинна бути поєднана із загальною стратегією підприємства.

Як показує аналіз діяльності вітчизняних суб'єктів агропродовольчої сфери, в сучасних умовах потреба у формуванні та реалізації стратегії інформаційної безпеки, як правило, виникає у аграрних підприємств, які мають досить значні конкурентні положення на ринку, які визначили довгострокові перспективи власного розвитку, але зіткнулися з такими викликами: недостатній рівень інформаційної безпеки ключових бізнес-процесів підприємства; відсутність взаємозв'язку між стратегічними цілями підприємства і напрямками розвитку інформаційної безпеки; низька віддача від інвестицій в розвиток інформаційної безпеки [1, 4, 5, 7, 10, 11, 12].

Визначення особливостей формування стратегії інформаційної безпеки необхідно починати з виявлення суб'єктів, зацікавлених у забезпеченні своєчасного доступу до необхідного масиву інформації, конфіденційності певної частини інформації, достовірності інформації, захисту частини інформації від незаконного її тиражування, розмежування відповідальності за порушення законних прав інших суб'єктів інформаційних відносин і встановлених правил поводження з інформацією, можливості здійснення безперервного контролю й управління процесами обробки та передачі інформації. Зацікавлені сторони у розробці та реалізації інформаційної стратегії підприємства потрібно розподілити на внутрішні та зовнішні, карта інтересів яких відображена на рис. 1.

З точки зору бізнесу, інформаційні технології є інструментом, які підтримують існуючі бізнес-процеси, відповідно, на кінцевий стан інформаційної безпеки агарного підприємства, в першу чергу, впливає бізнес-стратегія підприємства. Таким чином процес формування стратегії захисту інформації повинен перебувати у тісному взаємозв'язку з основними бізнес-цілями підприємства та його загальною стратегією (рис. 2). Відповідно до запропонованої моделі формування стратегії інформаційної безпеки на основі взаємозв'язку з бізнес-стратегією підприємства, основою зазначеного процесу є визначення базових елементів забезпечення інформаційної безпеки підприємства: перелік недоліків і вразливостей відповідно до проведеного контролю, перелік направлень розвитку бізнесу, перелік дій відповідно до внутрішніх факторів, результати визначення ролі та пріоритетності інформаційної безпеки підприємства, результати оцінки інформаційних ризиків, актуальні тенденції та кращі практики розвитку інформаційної безпеки, вплив зацікавлених сторін.

Рис. 1. Зацікавлені сторони у формуванні та реалізації стратегії інформаційної безпеки аграрного підприємства (сформовано автором на основі [7])

На основі визначення та взаємного врахування бізнес-напрямів розвитку підприємства та напрямів розвитку інформаційної безпеки визначаються стратегічні напрями управління інформаційною безпекою та цілі в межах кожного напряму (ціль М). В разі, якщо досягнення цілі призводить до отримання понад очікуваного ефекту, то в такому разі вона визначається як «надціль» (ціль М+1).

Враховуючи зазначені базові елементи забезпечення інформаційної безпеки підприємства доцільно виділити 8 основних типів стратегій управління захистом інформації (табл. 1).

З огляду літератури також було визначено два основні аспекти стратегій інформаційної безпеки агарного підприємства: час та простір. Із «часової» точки зору, стратегії можуть бути спрямовані на очікування нападу або реагування після нападу. З «просторової» точки зору, стратегії захисту інформації можуть розподілятися на такі, що спрямовані на захист всієї інформаційної системи, або на захист окремих інформаційних об'єктів. Важливою також є класифікація стратегій з точки зору прийняття рішень, що передбачає визначення конкретної тактики захисту на інформаційні атаки.

Рис. 2. Процес формування стратегії інформаційної безпеки на основі взаємозв'язку з бізнес-стратегією підприємства (сформовано автором на основі [7])

Узагальнюючи розглянуті стратегії, доцільно відзначити, що основними напрямами захистку інформації при реалізації будь-якого типу стратегії інформаційної безпеки підприємства агропродовольчого сектору повинні стати:

- ❖ основні принципи формування переліку критичних ресурсів, які потребують захисту, що формується в процесі проведення аудиту безпеки та аналізу ризиків. Даний перелік повинен включати в себе опис фізичних, програмних та інформаційних ресурсів з визначенням вартості ресурсів і ступеня їх критичності для підприємства;
- ❖ основні принципи захисту, що визначають стратегію забезпечення інформаційної безпеки та перелік правил, якими необхідно керуватися при побудові системи забезпечення інформаційної безпеки підприємства;
- ❖ модель порушника безпеки, яка визначається на основі обстеження ресурсів системи і способів їх використання;
- ❖ модель загроз безпеки та оцінку ризиків, пов'язаних з їх здійсненням, що формується на основі переліку критичних ресурсів і моделі порушника, яка включає визначення ймовірностей загроз й способів їх здійснення, а також оцінку можливих збитків;
- ❖ вимоги безпеки, які визначаються за результатами аналізу ризиків;
- ❖ заходи забезпечення безпеки організаційного та програмно-технічного рівня, що вживаються для реалізації перерахованих вимог;
- ❖ відповідальність співробітників підприємства за дотримання встановлених вимог інформаційної безпеки при експлуатації інформаційної системи підприємства [2, 4, 12].

Таблиця 1. Напрямів формування стратегії інформаційної безпеки аграрного підприємства (сформовано на основі [6, 7, 10, 11])

Тип стратегії	Характеристика стратегії
Профілактична стратегія (превентивна) (Prevention)	Профілактика спрямована на захист інформаційних активів до нападу шляхом заборони несанкціонованого доступу, модифікації, знищення чи розголошення. Найчастіше використовується запобіжний контроль – автентифікація, яка спрямована на обмеження доступу до авторизованих користувачів. Подальші профілактичні методи включають використання програмного забезпечення, яке регулює взаємодію користувачів з інформаційними активами, шифруючи інформацію щоб запобігти витоку.
Стратегія стримування (Deterrence)	Розглядає людину (персонал) як основне джерело загроз інформаційній безпеці. Передбачає здійснення дисциплінарних дії з метою впливу на поведінку людини (працівника) стосовно використання інформаційних активів підприємства. Один з головних привілеїв застосування стратегії стримування – це реалізація політики безпеки, яка передбачає конкретизацію покарання працівників, які це застосовують і не дотримуються правил інформаційної безпеки.
Стратегія спостереження (Surveillance)	Передбачає систематичний моніторинг середовища безпеки, спрямований на формування ситуаційної обізнаності з метою адаптації до мінливих обставин та виникаючих загроз, що визначає можливість вчасно попередити, або уникнути інцидентів інформаційної безпеки та розробити більш ефективні засоби захисту. Моніторинг середовища інформаційної безпеки підприємства у фізичній та цифровій сферах за допомогою технічних і нетехнічних засобів є складним завданням. Стратегія передбачає реєстрацію доступу до обмежених фізичних та логічних просторів, де зберігається інформація про копіювання та програмне забезпечення тощо.
Стратегія виявлення (Detection)	Виявлення – це стратегія операційного рівня, спрямована на виявлення конкретної безпеки. Зазначена стратегія контрастує із стратегією нагляду. Проте, виявлення фокусується на конкретній події, тоді як спостереження визначає загальну ситуацію інформаційної захищеності. Виявлення має різні форми: виявлення шкідливої або незвичної поведінки працівників, вторгнення чи несанкціоноване використання інформаційних ресурсів, програмних, апаратних засобів тощо.
Стратегія реагування (відповіді) (Response)	Стратегія реагування передбачає реалізацію відповідних коригувальних дій щодо виявлених атак. Відповідь на напад можна розділити на дві фази. По-перше, фаза реакції, де вживаються відповідні дії проти нападника або атаки і, по-друге, фаза відновлення, коли пошкоджену систему повертають до початкового стану. Однією з тактик стратегії реагування є стримування, яке відокремлює нападника або атаковану сферу від інших областей.
Стратегія відволікання (стратегія «обману») (Deception)	Стратегія «обману» відволікає увагу зловмисника від критично важливих інформаційних активів, використовуючи «приманки», що змушує порушника втрачати час та ресурси, а систему захисту забезпечити створити умови безпеки інформаційних ресурсів. Обман має два конструкти: пасивний обман та активний обман. Пасивний обман зосереджується на тому, щоб щось приховувати, тоді як активний обман зосереджується на тому, щоб щось показати. Обговорено два види манок – програмні манки та «медові горщики». Програмні манки являють собою обгортку, яка спілкується з процесами виклику або потоками від імені критичного програмного забезпечення. «Медові горщики» призначені для зловмисників несанкціонованого доступу, переконуючи їх у тому, що система є реальною і цінною ціллю.
Стратегія захисту по периметру (Perimeter Defense)	Периметр – це «фізична або логічна межа, визначена для домену, в межах якої визначена політика безпеки або застосовується архітектура безпеки» (Shirey 2007). В умовах інформаційної безпеки захист периметра передбачає створення межі навколо інформаційних активів, яка забезпечується регулюванням трафіку на кожному вхідному та вихідному інформаційному каналі. Мережеві брандмауери, механізми контролю доступу, механізми аутентифікації, контрзаходи проти (розповсюдженого) відмови у службових атаках – типові засоби управління, що реалізуються як основа стратегії оборони периметра.
Стратегія компартменталізації (Compartmentalization)	Компартменталізація зменшує можливості зловмисників, поділяючи визначену область атаки на окремі захищені зони. Таким чином, в разі, якщо зловмисник, який подолав захист однієї зони, автоматично не має доступу до інших зон. Інформаційні активи класифікуються на категорії: таємні та надтаємні. Кожній одиниці персоналу призначаються права доступу до окремих категорій інформації. Типовим прикладом цієї стратегії є DMZ (демілітаризована зона) або мережева зона, ізольована від внутрішньої мережі, але відкрита для загального доступу.
Стратегія шарування (layer)	Шарування використовує безліч контрзаходів, які функціонують незалежно один від одного, але підвищують загальну ефективність захисту в разі комплексної взаємодії. Пошаровий захист ґрунтується на переконанні, що єдиної стратегії недостатньо, тому потрібний складний набір інтелектуальних та інноваційних технологій інформаційного захисту.

Як було зазначено, базовим і важливим елементом формування стратегії захисту інформаційних об'єктів є використання перевірених практик та актуальних тенденцій розвитку інформаційної безпеки підприємств, серед яких слід виділити: власне тенденції розвитку інформаційної безпеки, заходи та технології (рис. 3).

Рис. 3. Практики оптимізації та актуальні тенденцій розвитку системи інформаційної безпеки підприємства (сформовано автором на основі [1, 7, 10])

Отже, на основі зазначеного, доцільно відзначити, що стратегія інформаційної безпеки аграрних підприємств – це структурований і взаємопов'язаний набір виважених дій, спрямованих на довгострокову перспективу захисту інформаційних об'єктів підприємства.

Стратегію інформаційної безпеки варто розглядати як карту, яка визначає орієнтири досягнення безпечних умов протікання основних управлінських та виробничих процесів суб'єктів агропродовольчої сфери та дозволяє забезпечити отримання економічного та соціального ефекту [8]. При цьому, варто звернути увагу, що стратегія інформаційної безпеки не повинна бути статичною і, в міру зменшення фактору невизначеності з плином часу, стратегія повинна переглядатися і, при необхідності, коригуватися, задаючи нові пріоритети прийняття тактичних рішень.

Висновки та перспективи подальших розвідок

Зважаючи на розвиток агропродовольчої сфери, його постійну інформатизацію, цифровізацію й автоматизацію, проблеми захисту інформації суб'єктів зазначеного сектору набувають стратегічного значення. Проведене дослідження дало змогу визначити сутність інформаційної стратегії аграрних підприємств як структурованого і взаємопов'язаного набору виважених дій, спрямованих на довгострокову перспективу захисту інформаційних об'єктів підприємства.

Визначення основних елементів формування та реалізації інформаційної стратегії аграрних утворень, зацікавлених сторін у формуванні та реалізації стратегії

інформаційної безпеки аграрного підприємства, характеристика типів інформаційних стратегій, актуальні тенденції та кращі практики розвитку інформаційної безпеки підприємства дозволить досліджуваним підприємствам обрати оптимальну інформаційну стратегію, яка буде взаємообумовленою загальною стратегією розвитку, та сформувати необхідний набір програмних, технічних, апаратних та організаційних інструментів захисту інформаційних ресурсів.

Список літератури

1. Адаптивные стратегии информационной безопасности. Экономика и жизнь. 2018. URL: https://www.eg-online.ru/article/365352/
2. Бирюков В. А., Лихарев Н. С. Стратегия информационной безопасности медиаорганизации. *Вестник МГУП.* 2015. №3. URL: https://cyberleninka.ru/article/n/strategiya-informatsionnoy-bezopasnosti-mediaorganizatsii
3. Євсеєв С. П. Дисертація методологія побудови системи безпеки банківських інформаційних ресурсів: дис. … ступеня д-ра тех. наук : 21.05.01 / Національний авіаційний університет. Київ, 2018. 471 с.
4. Левков Я. Разработка стратегии и архитектуры информационной безопасности предприятия. 2011. URL: https://profit.kz/articles/1700/Razrabotka-strategii-i-arhitekturi-informacionnoj-bezopasnosti-predpriyatiya/
5. Перун Т. С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні : автореф. дис. на здобуття наук. ступеня к-та юрид. наук: 12.00.07. Львів, 2019. 23 с.
6. Построения системы информационной безопасности. Основные аспекты построения системы информационной безопасности. URL: https://www.intuit.ru/studies/courses/13845/1242/lecture/27501
7. Чаплыгин Р. Стратегия информационной безопасности. URL: https://docplayer.ru/43503819-Strategiya-informacionnoy-bezo pasnosti.html
8. Чередниченко А. О. Організаційно-економічне забезпечення управління інформаційною безпекою підприємств будівельної галузі: автореф. дис. на здобуття наук. ступеня к-та екон. наук: 21.04.02. Харків, 2016. 24 с.
9. Anderson E. E., Choobineha J. Enterprise information security strategies. C*omputers & Security.* 2018*.* №8. P. 22-29.
10. Atif A., Maynard S. B., Park S. Information security strategies: towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing.* 2014. 25(2). URL: https://www.researchgate.net/publication/257580942.
11. Tapiador J. E., Clark J. A. Masquerade mimicry attack detection: a randomised approach. *Computers and Security.* 2011. №30 (5). P. 297-310.
12. Williamson M. M. Resilient Infrastructure for Network Security. *Complexity*. 2004. № 9 (2). P. 34-40.

References

1. Adaptivnyye strategii informatsionnoy bezopasnosti [Adaptive information security strategies]. *Ekonomika i zhizn'.* Available at: https://www.eg-online.ru/article/365352/
2. Biryukov, V. A., Likharev, N. S. (2015). Strategiya informatsionnoy bezopasnosti mediaorganizatsii [Information security strategy for a media organization]. *Vestnik MGUP.* No 3. Available at: https://cyberleninka.ru/article/n/strategiya-informatsionnoy-bezopasnosti-mediaorganizatsii

3. Evseev, S. P. (2018). Dysertatsiya metodolohiya pobudovy systemy bezpeky bankivs'kykh informatsiynykh resursiv. [The dissertation methodology of building the security system of banking information resources]. D. Sc. Thesis: 21.05.01 / National Aviation University. Kyiv. Ukraine.
4. Levkov, I. (2011). Razrabotka strategii i arkhitektury informatsionnoy bezopasnosti predpriyatiya. [Development of a strategy and architecture of information security of the enterprise]. Available at: https://profit.kz/articles /1700/Razrabotka-strategii-i-arhitekturi-informacionnoj-bezopasnosti-predpriyatiya/
5. Perun, T. S. (2019). Administratyvno-pravovyy mekhanizm zabezpechennya informatsiynoyi bezpeky v Ukrayini. [Administrative and legal mechanism of information security in Ukraine]. Abstract of Ph.D. Thesis: 12.00.07. Lviv. Ukraine.
6. Postroyeniya sistemy informatsionnoy bezopasnosti. Osnovnyye aspekty postroyeniya sistemy informatsionnoy bezopasnosti. [Building an information security system. The main aspects of building an information security system]. Available at: https://www.intuit.ru/studies/courses/13845/1242/lecture/27501
7. Chaplygin, R. Strategiya informatsionnoy bezopasnosti. [Information Security Strategy]. Available at: https://docplayer.ru/43503819-Strategiya-informacionnoy-bezo pasnosti.html
8. Cherednichenko, A. A. (2016). Orhanizatsiyno-ekonomichne zabezpechennya upravlinnya informatsiynoyu bezpekoyu pidpryyemstv budivel'noyi haluzi [Organizational and economic support of information security management in the construction industry]. Abstract of Ph.D. Thesis: 21.04.02. Kharkiv. Ukraine.
9. Anderson, E. E., Choobineha J. (2017). Enterprise information security strategies. C*omputers & Security,* no 8. pp. 22-29.
10. Atif, A., Maynard, S. B., Park, S. (2014). Information security strategies: towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing.* no 25(2). Available at: https://www.researchgate.net/publication /257580942.
11. Tapiador, J. E., Clark, J. A. (2011). Masquerade mimicry attack detection: a randomised approach. *Computers and Security.* no 30(5). pp. 297-310.
12. Williamson, M. M. (2004). Resilient Infrastructure for Network Security. *Complexity*. no 9 (2). pp. 34-40.

Стаття надійшла до редакції 05.09.2019 р.