УДК 004.056:331.58:331
JEL O33, F42
DOI 10.32782/2786-765X/2023-1-5

Мазник Л.В.
кандидат економічних наук
доцент кафедри економіки праці та менеджменту
Національний університет харчових технологій
ORCID: https://orcid.org/0000-0002-5387-7442
Драган О.І.
доктор економічних наук,
професор кафедри економіки праці та менеджменту
Національний університет харчових технологій
ORCID: https://orcid.org/0000-0002-7606-2385

ІНФОРМАЦІЙНА БЕЗПЕКА ОРГАНІЗАЦІЇ ЯК ФАКТОР ПОСИЛЕННЯ БРЕНДУ РОБОТОДАВЦЯ

В статті розглядаються питання актуальності формування та посилення бренду роботодавця в умовах посилення конкурентної боротьби за таланти та зростаючих ризиків в сфері інформаційної безпеки в умовах повномасштабної війни. Авторами визначені ключові елементи, які є основою бренду роботодавця з урахуванням вимог інформаційної безпеки. Зазначено, що головним напрямком забезпечення інформаційної безпеки є створення комплексної системи захисту інформації, що передбачає комплекс і технічних та організаційних заходів. Розглянуті питання сертифікації систем управління інформаційною безпекою як індикатора ефективності управління бізнес-процесами організації, інформаційними ризиками, стійкості та надійності розвитку компанії. Запропоновано послідовність дій для впровадження стандартів інформаційної безпеки та систему метрик оцінки ефективності впровадження стандартів інформаційної безпеки як факторів посилення бренду роботодавця. В роботі обґрунтовано, що при формуванні ціннісної пропозиції роботодавця (EVP) доцільно додавати до набору переваг дотримання стандартів інформаційної безпеки.

Ключові слова: бренд роботодавця, інформаційна безпека, репутація, стандарти, комплексна система захисту інформації, система управління інформаційною безпекою.

Постановка проблеми. Займатися формуванням бренду роботодавця стає все більш важливою задачею в наш час з кожним днем. Це пов'язано з тим, що конкуренція серед підприємств за висококваліфікованих працівників далі зростає, а це означає, що компанії повинні бути привабливими для залучення зацікавлених кандидатів на вакансії.

Більшість практикуючих експертів в сфері HR визначають бренд роботодавця (employer brand) як репутацію компанії як роботодавця, що має на меті надати кандидатам відповіді на запитання, чому варто працювати саме в цій організації, без прив'язки до конкретної ролі та чому співробітники компанії мають продовжувати працювати в ній (лояльність). Відповіді на ці питання містяться в результатах врахування всіх аспектів діяльності організацій, в тому числі і інформаційного.

Належний рівень інформаційної безпеки відіграє важливу роль у формуванні бренду роботодавця, до того ж слід врахувати нові ризики, які виникають при використанні інформаційних систем у воєнний час. Якщо підприємство піклується про безпеку своїх даних і дані своїх працівників і демонструє цей принциповий підхід до виконання цієї задачі, то збільшується довіра до компанії з боку працівників та клієнтів. Це може зробити підприємство більш привабливим для працівників, інші люди шукають роботодавців, які гарантують їхню безпеку та захищеність на робочому місці.

Отже, інформаційна безпека є необхідною умовою для формування успішного бренду роботодавця. Компанії, які вміють належним чином захищати свою інформацію, будуть привабливими для талановитих працівників та клієнтів, що може позитивно вплинути на їхні результати та розвиток.

Аналіз останніх досліджень і публікацій. Існує дуже значний доробок вчених і практиків в сфері створення, розвитку та управління брендом роботодавця, але на аспекти інформаційної безпеки як одного з ключових факторів, що забезпечують його посилення, окремо не досліджені. В статті Фірсової С.Г., Кожухівської А.О. [1] наголошується, що розвиток бренду роботодавця є невід'ємною частиною бізнес-стратегії підприємства. В дослідженні Gontareva I., Tymoshenko K. [2] відзначено, що формування бренду роботодавця – це стратегічний процес, використана дуже корисна методика оцінювання бренду на основі проведення опитувань. В роботі Buchelt B., Ziębicki

B., Jończyk J. [3] зазначається, що польські постачальники медичних послуг стикаються з дефіцитом людських ресурсів, а для залучення та утримання медичного персоналу в якості ефективних заходів пропонується розвиток діяльності з брендингу роботодавця, оскільки це призводить до покращення репутації організації та практики управління персоналом. Автори дослідження [4] пов'язують розвиток внутрішнього бренду шведських роздрібних компаній з організаційною стійкістю.

Українські підприємства стикнулись із необхідністю вести бізнес в умовах воєнного стану. Частиною агресії росії є створення інформаційних небезпек, тобто ускладнень і викликів стає все більше. Тому нам необхідно враховувати в своїй діяльності відповідні вимоги до захисту інформації. У «Вимогах до захисту інформації в інформаційних системах у воєнний час: роз'яснення Держспецзв'язку» [5] наголошується на відсутності певних специфічних заходів щодо дотримання інформаційної безпеки у воєнний час, всі вимого встановлені в Законі України «Про захист інформації в інформаційно-комунікаційних системах» [6]. Всі інформаційні системи, вимоги до захисту яких закріплені в законодавстві України, мають бути захищені за чинними стандартами. В цьому документі наголошується, що інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, мають оброблятися в системі із застосуванням комплексної системи захисту інформації (КСЗІ) з підтвердженою відповідністю. Підтвердження відповідності комплексної системи захисту інформації здійснюється за результатами державної експертизи, яка проводиться з урахуванням галузевих вимог і норм інформаційної безпеки у порядку, встановленому законодавством.

Метою статті є обґрунтування необхідності впровадження відповідних стандартів інформаційної безпеки, проходження сертифікаційних процедур з урахуванням сучасних реалій функціонування українських підприємств, що сприятиме посиленню бренду роботодавця.

Виклад основного матеріалу дослідження. Існує кілька ключових елементів, які є основою бренду роботодавця:

1. Культура підприємства (система цінностей, переконань і підходів, які формують робоче середовище в компанії).

2. Репутація компанії (ставлення громадськості, співробітників та клієнтів до компанії. Це не лише репутація на ринку продуктів та послуг, але й як компанія ставиться до своїх працівників).

3. Професійний розвиток (навчання та створення можливостей для своїх працівників щодо кар'єрного зростання).

4. Комунікація зі співробітниками (компанії повинні забезпечити відкритість та прозору комунікації зі своїми працівниками).

5. Безпека та охорона здоров'я (важливо, щоб компанія забезпечувала безпечні робочі умови та захист від небезпек).

6. Баланс роботи та особистого життя (компанії можуть забезпечити графік роботи та інші переваги, які дозволяють працівникам балансувати між професійним та особистим життям).

7. Соціальна відповідальність (компанії можуть виконувати соціально відповідальні проекти та ініціативи із сприяння розвитку соціальних, економічних та екологічних проєктів).

Ці елементи допомагають сформувати повну картину бренду роботодавця компанії і залежно від того, чим кожен з них позначається, можна підвищити привабливість компанії для потенційних працівників. Але в цьому переліку не акцентовано увагу на дуже важливій складовій бренду роботодавця – інформаційній безпеці.

В документі [5] зазначено, що системи захисту інформації є першим кордоном, що стримує ворога від знищення нашої країни в кіберпросторі. Витік персональних даних українців загрожує тим, що військові та спецслужби ворога можуть використати і використовують їх проти нашого населення. Витік чутливих даних збільшує ризики в роботі органів влади та критичної інфраструктури. Таким чином, під час повномасштабної війни та протистояння російській агресії питання захисту даних в інформаційних системах постає більш гостро. Отже, формування комплексної системи захисту інформації як сукупності технічних та організаційних заходів захисту впроваджуються як в інформаційній системі власника у вигляді технічних (програмно-апаратних та програмних) засобів захисту та їх налаштувань, так і в установі власника у вигляді розпоряджень, планів, інструкцій, методик, що будуються на відповідних стандартах. Побудовою комплексної системи захисту інформації можуть займатися як спеціалізовані організації, так і самі компанії, якщо у них є відповідні фахівці за умови, що відповідна система відповідає усім законодавчо встановленим вимогам і змогла отримати атестат відповідності. Документом, що засвідчує відповідність стандартам є атестат відповідності комплексної системи захисту інформації, який видається за результатом проведення державної експертизи у сфері технічного захисту інформації. Така експертиза проводиться відповідно до «Положення про державну експертизу у сфері технічного захисту інформації» [7].

Експертиза проводиться організатором експертизи (установою, яка має відповідну ліцензію) на договірних засадах, які у тому числі передбачають і терміни проведення робіт, що залежать від складності системи, досвіду експертів, якості побудови та документування відповідної комплексної системи захисту інформації. За позитивними результатами експертизи Адміністрацією Держспецзв'язку реєструється атестат відповідності комплексної системи захисту інформації.

Для захисту інформаційних систем, в яких не обробляється інформація з обмеженим доступом, але захист яких вимагає українське законодавство, може бути також використана альтернативна система інформаційної безпеки відповідно до європейських стандартів ISO/IEC 27 серії. Ці стандарти передбачають систему управління інформаційною безпекою (СУІБ) як елемент загальної системи управління, що ґрунтується на врахуванні ризиків інформаційної безпеки в якості бізнес-ризиків. Ця система призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки. Для процесів СУІБ застосовується модель «плануй-виконуй-перевіряй-дій» (ПВПД; англ. *Plan-Do-Check-Act, PDCA*): Plan (планування) – фаза створення СУІБ, створення переліку активів, оцінки ризиків та вибору заходів; Do (дія) – етап реалізації та впровадження відповідних заходів; Check (перевірка) – фаза оцінки ефективності та продуктивності СУІБ. Зазвичай виконується внутрішніми аудиторами; Act (поліпшення) – виконання превентивних і коригуючих дій).

Отже, важливо, що крім розробки правил управління та забезпечення безпеки, не менш важливо забезпечити циклічність всіх процесів управління безпекою, щоб всі процедури послідовно проходили етапи моделі PDCA. Саме це є свідченням відповідності системи управління стандарту ISO 27001 та доводить готовність до сертифікації СУІБ. Виконання вимог стандарту ISO/IEC 27001 переважно дозволяє мінімізувати ризики втрат активів організації, а отже скоротити ризики фінансових втрат.

Сертифікація системи управління інформаційною безпекою – це ефективне управління бізнес-процесами організації, інформаційними ризиками, а також засвідчує стійкість та надійність розвитку компанії. Що, в свою чергу, забезпечує позитивне ставлення бізнес-партнерів. СУІБ відповідно до стандарту ISO/IEC 27001 – це частина загальної системи менеджменту компанії. Сімейство стандартів ISO 27000 включає в себе документи, які стосуються систем управління інформаційною безпекою:

ISO/IEC 27001 Information security management systems. Requirements – Системи управління інформаційною безпекою. Вимоги.

ISO/IEC 27000 Information security management systems. Overview and vocabulary – Системи управління інформаційної безпеки. Огляд та термінологія.

ISO/IEC 27003 Information Security Management Systems. Guidance – Системи управління інформаційної безпеки. Посібник.

ISO/IEC 27004 Information security management. Measurement – Вимірювання ефективності системи управління інформаційної безпеки.

ISO/IEC 27006 Requirements for bodies providing audit and certification of information security management systems – Вимоги до органів, які здійснюють аудит та сертифікацію систем менеджменту інформаційної безпеки.

ISO/IEC 27007 Guidelines for Information Security Management Systems auditing (FCD) – Посібник для аудиту систем управління інформаційною безпекою.

Прийняття стандартів інформаційної безпеки може підвищити привабливість компаній для працівників, які працюють у компаніях, які забезпечують безпеку їхньої конфіденційної інформації. Ось декілька стандартів інформаційної безпеки, впровадження яких може призвести до зміцнення бренду роботодавця:

1. ISO 27001: це міжнародний стандарт, який організація може використовувати для керування своєю інформаційною безпекою. Вихідні принципи цього стандарту допомагають компаніям захищати свою конфіденційну інформацію, регулювати доступ до неї та забезпечувати дотримання правил.

2. GDPR: Це Загальний регламент про забезпечення захисту даних, що регулює збір, зберігання та переробку даних в Європейському Союзі. Цей стандарт компанії забезпечує захист персональних даних своїх працівників та клієнтів, що може збільшити репутацію компанії в очах наявних працівників [8].

3. HIPAA: це стандарт, який використовується організаціями з охорони здоров'я допомагають їм захищати конфіденційну медичну інформацію своїх користувачів. Якщо компанія дотримується стандартів HIPAA, це можна позитивно вплинути на репутацію компанії, яка включає до соціального пакету послуги медичного страхування працівників [9].

4. PCI DSS: це стандарт, який використовують до компаній, які збирають, обробляють і зберігають кредитну інформацію. Основним обов'язком таких компаній є захист конфіденційних даних своїх клієнтів та збільшення їх довіри до компанії [10].

Отже, прийняття стандартів інформаційної безпеки може допомогти компанії зміцнити свій бренд роботодавця, забезпечуючи безпеку конфіденційності інформації своїх співробітників і клієнтів.

Для впровадження стандартів інформаційної безпеки в компанії слід дотримуватись наступного алгоритму:

1. *Оцінка потреби компанії в інформаційній безпеці:* вибір конфіденційної інформації, яку потрібно захистити, визначення рівня доступу до неї.

2. *Визначення зон ризику:* вибір слабких місць в системах компанії, які можуть бути атаковані, визначення потенційних можливостей захисту.

3. *Розробка плану впровадження:* створення детального плану для всієї компанії, який забезпечить уніфікацію стандартів інформаційної безпеки для всієї компанії.

4. *Організація навчання:* забезпечення навчання для всіх працівників компанії, щоб вони були знайомі з принципами інформаційної безпеки та допомагали захистити конфіденційну інформацію.

5. *Створення контрольного списку:* для оперативного контролю дотримання стандартів інформаційної безпеки у всіх підрозділах.

Щодо оцінки ефективності впровадження стандартів інформаційної безпеки, можна використовувати наступні метрики:

1. Кількість порушень безпеки: вимірюється кількість порушень безпеки, які сталися в компанії після впровадження стандартів інформаційної безпеки.

2. Час відновлення: вимірюється час, необхідний для відновлення нормальної роботи після порушення безпеки.

3. Кількість працівників, що пройшли відповідне навчання щодо стандартів інформаційної безпеки.

4. Кількість вірусів і шкідливих програм: вимірюється кількість вірусів і шкідливих програм, знайдених на комп'ютерах в компанії після впровадження стандартів інформаційної безпеки.

Якщо впровадження стандартів інформаційної безпеки буде ефективним, компанія зможе підвищити свій бренд як роботодавця, забезпечивши надійний захист конфіденційної інформації.

В ході ознайомлення із існуючими стандартами інформаційної безпеки виникли деякі додаткові ідеї щодо їх впровадження та оцінки ефективності результатів такого впровадження:

Розробка контрольного списку вимог безпеки: одним із перших кроків у впровадженні стандартів інформаційної безпеки є розробка контрольного списку вимог безпеки. Це допоможе визначити вразливі місця організації та визначити, як їх усунути.

Впровадження ефективних загальноорганізаційних програм управління ризиками. Ефективне управління ризиками є важливою частиною будь-якої програми інформаційної безпеки. Це передбачає виявлення, оцінку та визначення пріоритетів ризиків і вжиття заходів для їх пом’якшення.

Оцінка третьою стороною стандартів інформаційної безпеки. Експерти можуть використовувати різні методи для оцінки ефективності стандартів інформаційної безпеки, включаючи оцінку третьою стороною. Це може передбачати наймання зовнішньої організації для проведення оцінки безпеки та надання рекомендацій щодо покращення.

Формування EVP (*Employee Value Proposition*), або ціннісної пропозиції роботодавця з додаванням до набору переваг, які допомагають кандидату відповісти на запитання *«Чому мені потрібно працювати саме у вашій компанії?»*, дотримання стандартів інформаційної безпеки.

Щоб створити ефективну ціннісну пропозицію роботодавця (EVP), яка враховує вимоги інформаційної безпеки, організації можуть враховувати такі фактори:

Культура усвідомлення безпеки: Організації повинні прагнути створити культуру, орієнтовану на безпеку, яка підкреслює важливість інформаційної безпеки в усіх відділах. Сюди входить надання безпеці пріоритету згори до низу та проведення регулярних тренінгів із захисту даних для працівників.

Конкурентоспроможна зарплата та переваги: ключовим фактором у розвитку сильного EVP є пропозиція конкурентоспроможної зарплати та пакету переваг, який відповідає галузевим стандартам. Це може допомогти залучити та утримати кращих спеціалістів із сильними навичками захисту інформації.

Можливості розвитку кар’єри. Забезпечення співробітникам можливості розвитку кар’єри та чітких шляхів прогресу є важливим для тих, хто цікавиться інформаційною безпекою. Можна залучити навчання та сертифікацію, а також програми наставництва та лідерства.

Акцент на балансі між роботою та особистим життям. Співробітників приваблюють компанії, які приділяють значну увагу балансу між роботою та особистим життям і надають пріоритет ініціативам у сфері здоров’я, таким як гнучкий графік і вихідний час.

Забезпечення безпеки даних: це найважливіший аспект, який слід враховувати при розробці EVP, який наголошує на безпеці

інформації. Демонстрація безпечного робочого середовища та гарантування захисту персональних даних співробітників є важливим аспектом ефективного EVP, який відповідає вимогам інформаційної безпеки.

Беручи до уваги ці фактори та вирішуючи проблеми безпеки під час створення EVP, організації можуть залучити та утримати найкращих талантів, а також створити імідж надійного роботодавця, який надає пріоритет інформаційній безпеці.

Впроваджуючи стандарти інформаційної безпеки, організації можуть захистити конфіденційну інформацію та захистити себе від кіберзагроз. Важливо періодично оцінювати ефективність цих стандартів, щоб переконатися, що вони залишаються актуальними та ефективними для захисту організаційних даних.

Висновки. Для ефективного впровадження стандартів інформаційної безпеки в Україні та зміцнення іміджу роботодавця необхідно враховувати наступні аспекти:

– відповідність національним нормам: організації повинні забезпечити дотримання національних норм України, які стосуються інформаційної безпеки та конфіденційності даних. Це включатиме дотримання Закону України «Про захист персональних даних» та інших відповідних законодавчих актів;

– розуміння українського ринку: Розуміння нюансів українського ринку має вирішальне значення, оскільки це допоможе запровадити стандарти інформаційної безпеки, адаптовані до конкретних потреб організації та місцевих уподобань. Це може включати включення місцевих культурних особливостей, а також навчання працівників.

– співпраця з місцевими зацікавленими сторонами: організації можуть співпрацювати з місцевими зацікавленими сторонами, такими як експерти з IT-безпеки, державні установи та галузеві асоціації. Це дозволить їм залишатися в курсі останніх подій у галузі, використовувати передовий досвід галузі та налагоджувати відносини що підвищує їхню репутацію.

– прозорість і комунікація: організації повинні бути прозорими щодо своїх методів захисту інформації та чітко повідомляти про це своїм співробітникам, клієнтам та іншим зацікавленим сторонам. Це допоможе зміцнити довіру та захистити від шкоди репутації в разі порушення даних або інциденту безпеки.

Враховуючи ці фактори та впроваджуючи надійні стандарти інформаційної безпеки, організації в Україні можуть підвищити свою репутацію надійного роботодавця, підвищити лояльність клієнтів і зменшити ризики, пов’язані з кіберзагрозами.

Бібліографічний список

1. Фірсова С.Г., Кожухівська А.О. Стратегічні аспекти управління брендом роботодавця. *Ефективна економіка*. 2020. № 9. URL: http://www.economy.nayka.com.ua/?op=1&z=8178 DOI: https://doi.org/10.32702/2307-2105-2020.9.51
2. Gontareva I., Tymoshenko K. Methodical approach to the employer’s brand analysis on the case of it-companies. *Social Economics*, 2020. No. 58. P. 59–69. DOI: https://doi.org/10.26565/2524-2547-2019-58-08
3. Buchelt B., Ziębicki B., Jończyk J. et al. The enhancement of the employer branding strategies of Polish hospitals through the detection of features which determine employer attractiveness: a multidimensional perspective. *Hum Resour Health.* 2021. 19. No. 77. DOI: https://doi.org/10.1186/s12960-021-00620-0
4. Biedenbach G., Biedenbach T., Hultén P. et al. Organizational resilience and internal branding: investigating the effects triggered by self-service technology. *J Brand Manag.* 2022. No. 29. P. 420–433. DOI: https://doi.org/10.1057/s41262-022-00275-9
5. Вимоги до захисту інформації в інформаційних системах у воєнний час: роз’яснення Держспецзв'язку». URL: https://www.kmu.gov.ua/news/vymohy-do-zakhystu-informatsii-v-informatsiinykh-systemakh-u-voiennyi-chas-roziasnennia-derzhspetszviazku
6. Закон України «Про захист інформації в інформаційно-комунікаційних системах». URL: https://ips.ligazakon.net/document/Z008000?an=4764
7. Про затвердження Положення про державну експертизу у сфері технічного захисту інформації : Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16 травня 2007 року № 9. URL: https://ips.ligazakon.net/document/RE14087
8. GDPR General Data Protection Regulation. URL: https://gdpr-info.eu/#:~:text=General%20Data%20Protection%20Regulation%20GDPR
9. HIPAA. URL: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
10. PCI DSS. URL: http://surl.li/htaad

References

1. Firsova S.H., Kozhukhivs′ka A.O. (2020) Stratehichni aspekty upravlinnya brendom robotodavtsya. [Strategic aspects of employer brand management]. *Efektyvna ekonomika*, no. 9. Available at: http://www.economy.nayka.com.ua/?op=1&z=8178 DOI: https://doi.org/10.32702/2307-2105-2020.9.51

2. Gontareva I., & Tymoshenko K. (2020) Methodical approach to the employer's brand analysis on the case of it-companies. *Social Economics*, no. 58, pp. 59–69. DOI: https://doi.org/10.26565/2524-2547-2019-58-08
3. Buchelt B., Ziębicki B., Jończyk J. et al. (2021) The enhancement of the employer branding strategies of Polish hospitals through the detection of features which determine employer attractiveness: a multidimensional perspective. *Hum Resour Health,* 19, no. 77. DOI: https://doi.org/10.1186/s12960-021-00620-0
4. Biedenbach G., Biedenbach T., Hultén P. et al. (2022) Organizational resilience and internal branding: investigating the effects triggered by self-service technology. *J Brand Manag*, no. 29, pp. 420–433. DOI: https://doi.org/10.1057/s41262-022-00275-9
5. Vymohy do zakhystu informatsiyi v informatsiynykh systemakh u voyennyy chas: roz'yasnennya "Derzhspetszv'yazku". Available at: https://www.kmu.gov.ua/news/vymohy-do-zakhystu-informatsii-v-informatsiinykh-systemakh-u-voiennyi-chas-roziasnennia-derzhspetszviazku]
6. Zakon Ukrayiny "Pro zakhyst informatsiyi v informatsiyno-komunikatsiynykh systemakh". Available at: https://ips.ligazakon.net/document/Z008000?an=4764
7. Pro zatverdzhennya Polozhennya pro derzhavnu ekspertyzu u sferi tekhnichnoho zakhystu informatsiyi: Nakaz Administratsiyi Derzhavnoyi sluzhby spetsial′noho zv'yazku ta zakhystu informatsiyi Ukrayiny vid 16 travnya 2007 roku No. 9. Available at: https://ips.ligazakon.net/document/RE14087
8. GDPR General Data Protection Regulation Available at: https://gdpr-info.eu/#:~:text=General%20Data%20Protection%20Regulation%20GDPR
9. HIPAA. Available at: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.
10. PCI DSS. Available at: http://surl.li/htaad

Стаття надійшла до редакції 30.05.2023

Liana Maznyk
Candidate of Economics,
Associate Professor of the Department of
Labor Economics and Management
National University of Food Technologies
ORCID: https://orcid.org/0000-0002-5387-7442

Olena Dragan
Doctor of Economics,
Professor of the Department of
Labor Economics and Management
National University of Food Technologies
ORCID: https://orcid.org/0000-0002-7606-2385

INFORMATION SECURITY OF THE ORGANIZATION AS A FACTOR FOR STRENGTHENING THE EMPLOYER BRAND

The article examines the relevance of forming and strengthening the employer's brand in the context of increased competition for talent and growing risks in the field of information security in the context of a full-scale war. **Objective.** The object is international information security standards in Ukraine and strengthening the employer's brand. **Methods** of scientific knowledge: descriptive, abstract-logical, generalization, comparison. **Results.** The authors identified the key elements that are the basis of the employer brand, taking into account information security requirements. It is noted that the main direction of ensuring information security is the creation of a complex system of information protection, which includes a complex of technical and organizational measures. The issues of certification of information security management systems as an indicator of the effectiveness of management of the organization's business processes, information risks, stability, and reliability of the company's development are considered. A sequence of actions for the implementation of information security standards and a system of metrics for evaluating the effectiveness of information security standards as factors for strengthening the employer's brand are proposed. The paper substantiates that when forming the employer's value proposition (EVP) it is advisable to add compliance with information security standards to the set of advantages. **Scientific novelty.** For the implementation of information security standards in order to strengthen the company's employer brand, an algorithm is proposed, which consists of the following stages: 1. Assessment of the company's need for information security. 2. Determination of risk zones. 3. Development of an implementation plan. 4. Organization of training. 5. Creation of a checklist for compliance with information security standards in all divisions. **Practical significance.** To evaluate the effectiveness of the implementation of information security standards, the following metrics are proposed: 1. The number of security breaches. 2. Recovery time. 3. The number of employees who have undergone appropriate training. 4. Number of viruses and malware. Demonstrating a secure work environment and ensuring that employees' personal data is protected is an important aspect of an effective EVP that meets information security requirements.

Keywords: employer brand, information security, reputation, standards, comprehensive information protection system, information security management system.