https://doi.org/10.31891/2219-9365-2024-79-10
УДК 004.056.53

ТІТОВА Віра
Хмельницький національний університет
https://orcid.org/0000-0001-8668-4834
e-mail: titovav@khmnu.edu.ua
КЛЬОЦ Юрій
Хмельницький національний університет
https://orcid.org/0000-0002-3914-0989
e-mail: klots@khmnu.edu.ua
ВОЛИНЕЦЬ Віталій
https://orcid.org/0009-0006-7999-1290
mailto:volynets1026@gmail.com
ПЕТЛЯК Наталія
Хмельницький національний університет
https://orcid.org/0000-0001-5971-4428
e-mail: npetlyak@khmnu.edu.ua
ОГОРОДНИК Максим
Хмельницький національний університет
e-mail: maks737271@gmail.com

РОЗРОБЛЕННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИВАТНОГО ПІДПРИЄМСТВА

У даній роботі представлено методику формування політики інформаційної безпеки у приватному секторі. Проведено аналіз систем даних, представлено їх техніко-економічні характеристики та визначено основні проблеми та завдання захисту інформації. Проведено порівняльний аналіз методів та засобів захисту інформації на аналогічних об'єктах інформаційної діяльності. Вибрано та продемонстровано методи захисту інформації в корпоративній мережі компанії за допомогою адміністративних заходів із запобігання загрозам інформаційної безпеки.

Ключові слова: політика інформаційної безпеки, методи та засоби захисту інформації.

TITOVA Vira, KLOTS Yurii
Khmelnitskyi National University
VOLYNETS Vitalii
PETLIAK Nataliia, OHORODNYK Maksym
Khmelnitskyi National University

DEVELOPING THE INFORMATION SECURITY POLICY OF A PRIVATE ENTERPRISE

Based on the analysis of the main provisions of the information protection theory, it was established that in order to create an information security policy, it is necessary to develop a number of documents and instructions aimed at information protection. And in no case should stop at one method of information protection, otherwise data protection will be at risk. Data protection must be comprehensive. The comprehensive policy of information security covers the development, production and installation of technical means of protection, as well as regular inspections of the information equipment used. The development of this policy is as follows: identification of deficiencies in the company's current information protection; identification of types of threats that may arise as a result of deficiencies in the protection of information systems of the enterprise; selection of methods and ways of solving existing problems.

As a solution, a set of measures was developed, which consists of administrative decisions that regulate the possibility of information leakage due to the influence of the human factor. Based on the analysis of the main methods and means of information protection, it was established that organizational and legal methods and means of information protection should be aimed at countering threats to information security, reducing risks and effectively handling incidents in order to ensure a sufficient level of data protection for a long time. The evaluation of the effectiveness of the proposed measures through economic substantiation proved their feasibility of implementation in the organization.

Keywords: information security policy, methods and means of information protection.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Поява нових інформаційних технологій та розвиток потужних комп'ютерних систем для зберігання та обробки інформації підвищили вимоги до рівня захисту інформації та визначили необхідність розробки ефективних механізмів захисту інформації, сумісних із сучасними архітектурами зберігання даних.

Забезпечення захисту інформації на підприємстві – це безперервний процес, що включає контроль зовнішнього і внутрішнього середовища підприємства, організацію та проведення заходів щодо підтримки

стабільного функціонування локальної мережі та обчислювальної техніки, а також використання сучасних методів, що дозволяють мінімізувати втрати від витоку інформації. Для захисту інформації, як у мережі, так і на виробництві, компаніям необхідно сформувати певні правила та норми, що регламентують поведінку співробітників для забезпечення безпеки, а також описати технічні та програмні засоби захисту інформації. На це й спрямовано розроблення політики безпеки.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Політика інформаційної безпеки компанії зазвичай виражається в серії документів, що відображають вимоги до захисту даних і основні напрямки діяльності компанії щодо безпеки [1]. Існує три основні рівні розробки політики безпеки: верхній, середній і нижній [2].

На верхньому рівні політики безпеки даних організації необхідно: сформулювати та продемонструвати ставлення адміністрації підприємства до системи захисту інформації та відобразити основні цілі та завдання в цій галузі; розробити індивідуальні політики безпеки, інструкції та правила, за допомогою яких регулюються окремі питання; інформувати співробітників організації про основні завдання та пріоритети в галузі інформаційної безпеки.

Політика інформаційної безпеки середнього рівня використовується для відображення корпоративних підходів і вимог, таких як: використання інформаційних систем; телекомунікаційних та інформаційних технологій, методів і підходів до обробки інформації; учасників процесів обробки інформації, від яких залежить забезпечення захисту інформації на підприємстві.

Нижній рівень політики безпеки використовується для опису конкретних процедур і документів для забезпечення інформаційної безпеки на підприємстві.

Етапи розроблення політики безпеки в організації включають: виконання оцінки особистого ставлення до загроз безпеці з боку власників і співробітників підприємства; проведення аналізу потенційно важливих інформаційних активів підприємства; виявлення існуючих загроз безпеки підприємства з подальшою оцінкою ризиків.

Розглянемо основні елементи політики інформаційної безпеки підприємства [3-5]. Захист передбачає використання організаційних засобів захисту, визначених політикою безпеки підприємства. На першому етапі необхідно визначити межі, в яких функціонуватиме політика інформаційної безпеки компанії та встановити критерії оцінки її результатів.

На етапі аналізу ризиків інформації визначають пріоритети обраних засобів захисту з розподілом їх за ступенем важливості на підприємстві, ідентифікують уразливість активів підприємства та визначають збитки. Результати аналізу ризиків інформаційної безпеки підприємства будуть застосовуватися у вигляді основи для планування роботи системи інформаційної безпеки, вибору найефективнішої стратегії та тактики. Для підвищення ефективності політики безпеки застосовуються такі прийоми, як групове визначення з використанням атрибутів та мандатне керування доступом.

Багато підприємств використовують глобальні та локальні політики безпеки, засновані на принципах управління інформаційною безпекою. Глобальні політики інформаційної безпеки спрямовані на забезпечення захисту інформації на рівні бізнес-процесів підприємства, тоді як локальні політики формуються на рівні захисту даних підприємства [4-6].

Глобальна політика підприємства являє собою правила безпеки, що описують можливі взаємодії між об'єктами, які потребують захисту інформації. Локальні політики безпеки підприємства використовуються для налаштування засобів захисту інформації, реплікації налаштувань вузлів і подальших коригувань. Зазвичай, локальні політики безпеки підприємства містять правила, які регулюють з'єднання і змінюють конфігурацію мережних пристроїв.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Отже, на основі проведеного огляду можна зробити висновок, що для розроблення політики безпеки приватного підприємства необхідно вирішити такі завдання: оцінити поточний стан інформаційної безпеки підприємства; виявити порушення в захисті інформаційної безпеки, а також виявлення найімовірніших загроз інформації; розробити пропозиції щодо реалізації адміністративних заходів із запобігання загрозам інформаційної безпеки.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Для захисту даних приватного підприємства необхідно користувачів розділити на групи з відповідними правами:

- administrator – адміністратори мережі (створення та управління політиками інформаційної безпеки, глобальні налаштування мережі тощо);
- engineer – облікові записи для повсякденного обслуговування інформаційно-обчислювальної техніки;

- worker – обліковий запис стандартного користувача (співробітника організації) з обмеженими правами;
- guest – обмежений обліковий запис (у разі необхідності доступу не співробітників організації).

Для ідентифікації користувача потрібен унікальний запис кожного користувача, який включено до відповідної групи. Тим самим здійснюється розмежування доступу (табл. 1).

Таблиця 1

Групи користувачів та їхні права

Дії	Guest	Worker	Engineer	Administrator
Створення та зміни груп користувачів	Ні	Ні	Ні	Так
Зміна налаштувань мережі	Ні	Ні	Ні	Так
Підключення до мережі нових робочих станцій	Ні	Ні	Ні	Так
Зміна налаштувань серверів	Ні	Ні	Ні	Так
Зміна прав доступу	Ні	Ні	Ні	Так
Встановлення додатків та ПЗ	Ні	Ні	Так	Так
Доступ до Інтернету	Ні	Так	Так	Так
Доступ до корпоративної електронної пошти	Ні	Так	Так	Так
Доступ до корпоративного чату	Ні	Так	Так	Так
Можливість завантажувати файли	Ні	Ні	Так	Так
Запис файлів	"Мої документи"	"Мої документи", "Робочий стіл"	Будь-яка папка на робочому ПК	Будь-який ПК мережі
Підключення флеш-дисків, зовнішніх дисків.	Ні	Ні	Так	Так

Відправною точкою для визначення економічної ефективності запропонованого підходу є очевидне припущення: з одного боку, порушення інформаційної безпеки завдає певної шкоди; з іншого боку, забезпечення інформаційної безпеки коштує дорого. Загальна очікувана вартість захисту може бути виражена як сума вартості захисту та збитків від порушення. Очевидно, що оптимальним рішенням є розподіл коштів на захист інформації таким чином, щоб мінімізувати загальну вартість захисту [7].

Також зрозуміло, що економічна ефективність заходів з інформаційної безпеки визначається розміром відверненого збитку або розміром зниження ризиків для інформаційних активів організації.

Достатньо визначити лише рівень збитків, оскільки оптимальне рішення проблеми доцільного рівня витрат на захист полягає в тому, що цей рівень дорівнює рівню збитків, які очікуються в разі порушення безпеки. Як одна з методик визначення рівня витрат можливе використання такої емпіричної залежності очікуваних втрат (ризиків) R від і-ї загрози інформації [8-9]:

$$R_i = 10^{Ti+Li-4}, \tag{1}$$

де T_i – коефіцієнт, що характеризує можливу частоту виникнення відповідної загрози; L_i – коефіцієнт, що характеризує значення можливого збитку в разі її виникнення.

Сумарна вартість втрат визначається формулою:

$$R = \sum_{i=1}^{N} R_i , \tag{2}$$

де N – кількість можливих загроз інформаційним активам.

При розрахунку сумарного показника рекомендується виходити з того, що загрози конфіденційності, цілісності та доступності здійснюються порушником незалежно. Іншими словами, припускається, що цілісність інформації порушена діями порушника, але її зміст залишається невідомим порушнику (конфіденційність не порушена), а авторизовані користувачі все ще мають доступ до активу, хоча й у спотвореному вигляді.

Для прикладу розглянемо інформаційні активи приватної компанії (табл. 2). Розрахунки показують, що ризик економічних втрат для цієї компанії становить приблизно 1 080 000 гривень. З цього можна зробити висновок, що це дуже значні втрати для підприємства. Для того, щоб зрозуміти, наскільки ефективною є розроблена політика інформаційної безпеки, необхідно розрахувати показники економічної ефективності проєкту.

Таблиця 2

Величини втрат (ризиків) для інформаційних ресурсів до впровадження розробленої політики безпеки

Інформаційний актив	Загроза	Величина втрат (тис. грн.)
Проєктна документація, розроблена організацією	конфіденційності	100
	цілісності	500
	доступності	20
Особисті дані клієнта	конфіденційності	300
	цілісності	20
	доступності	20
Особисті відомості про співробітників	конфіденційності	100
	цілісності	10
	доступності	10
Сумарна величина втрат		**1 080**

Для проведення розрахунків необхідно отримати дані про передбачуваний розмір втрат (ризику) ключових інформаційних ресурсів після впровадження/модернізації інформаційної безпеки. Результати базуються на висновках експертних досліджень (див. табл. 3).

Таблиця 3

Величини втрат (ризиків) для інформаційних ресурсів після впровадження розробленої політики безпеки

Інформаційний актив	Загроза	Величина втрат (тис. грн.)
Проєктна документація, розроблена організацією	конфіденційності	10
	цілісності	50
	доступності	2
Особисті дані клієнта	конфіденційності	30
	цілісності	2
	доступності	2
Особисті відомості про співробітників	конфіденційності	10
	цілісності	1
	доступності	1
Сумарна величина втрат		**108**

Отже, можна зробити висновки, що впровадження розробленої політики безпеки дозволяє знизити можливі збитки в 10 разів, тобто витрати політики безпеки окупляться вже в першому кварталі. І це є зовсім невеликим навантаження на фінансову систему організації.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Аналіз основних положень теорії інформаційної безпеки показує, що для створення політики інформаційної безпеки необхідно розробити низку документів та інструкцій з метою захисту інформації. Крім того, захист інформації не повинен обмежуватися лише одним методом захисту інформації. Захист даних повинен бути комплексним. Комплексна політика захисту інформації поширюється на розробку, виготовлення та встановлення технічних засобів захисту, а також на регулярну перевірку інформаційного обладнання, що використовується.

Розробка такої політики включає в себе виявлення поточних недоліків інформаційної безпеки підприємства, визначення типів загроз, які можуть виникнути через недоліки в захисті інформаційних систем підприємства, а також вибір шляхів і засобів для вирішення існуючих проблем.

В якості рішення автори розробили комплекс заходів, що складається з адміністративних рішень, які регламентують можливість витоку інформації через вплив людського фактору. На основі аналізу основних методів та заходів захисту інформації встановлено, що організаційно-правові методи та заходи захисту інформації повинні бути спрямовані на протидію загрозам інформаційній безпеці, зниження ризиків, ефективне реагування на інциденти та забезпечення достатнього рівня захисту даних протягом тривалого часу.

Ефективність запропонованих заходів оцінено за допомогою економічного обґрунтування, що свідчить про їх доцільність в організації.

Література

1. Основи інформаційної безпеки: навчальний посібник/ В.А. Лужецький, А.Д. Кожухівський, О.П. Войтович. Вінниця: ВНТУ, 2013. 221 с.

2. ДСТУ ISO/IEC 27005:2019. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки/ Нац. стандарт України. Вид. офіц [Чинний від 2019-11-01]. Київ: ДП «УкрНДНЦ», 2019. 76 с.

3. Формування моделі політики інформаційної безпеки на основі концепцій “глибинного захисту/ Д.В. Дячков// Підприємництво і торгівля. 2019. № 25. С. 116-121.

4. Політика інформаційної безпеки в системах інформаційно-аналітичного забезпечення підтримки прийняття організаційних рішень / С.М. Чуруброва // Проблеми програмування. 2016. № 4. С. 97-103.

5. Розробка політики інформаційної безпеки комп’ютерного контролю знань/ Н. Кухарська// Вісник Львівського державного університету безпеки життєдіяльності. 2017. №16. С.34-39.

6. Політика інформаційної безпеки об’єкта/ Ю. Хохлачова// Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2012 р. Вип. 2 (24). С. 23-29.

7. Оцінювання ефективності рішень в системах захисту інформації/ В. Ю. Тітова, О. С. Андрощук, В. С. Орленко, І. М. Шевчук, В. С. Даценко // Вісник Хмельницького національного університету. Технічні науки. 2020. № 5. С. 307–310.

8. Комерційна діяльність. Навч. посібник/ Л.Г. Филевич, Л.О. Попова, О.М. Прядко, Т.Л. Мітяєва, Л.А. Прибилович. Харків: ХДУХТ, 2014. 225 с.

9. Інформаційна політика в системі забезпечення фінансової безпеки держави/ А.Д. Глушко, В.В. Пантась, С.Р. Бабенко// «Ефективна економіка». 2022. №2.

References

1. Osnovy informatsiinoi bezpeky : navchalnyi posibnyk/ V.A. Luzhetskyi, A.D. Kozhukhivskyi, O.P. Voitovych. Vinnytsia: VNTU, 2013. 221 s.

2. DSTU ISO/IEC 27005:2019. Informatsiini tekhnolohii. Metody zakhystu. Upravlinnia ryzykamy informatsiinoi bezpeky / Nats. standart Ukrainy. Vyd. ofits [Chynnyi vid 2019-11-01]. Kyiv: DP «UkrNDNTs», 2019. 76 s.

3. Formuvannia modeli polityky informatsiinoi bezpeky na osnovi kontseptsii “hlybynnoho zakhystu/ D.V. Diachkov// Pidpryiemnytstvo i torhivlia. 2019. № 25. S. 116-121.

4. Polityka informatsiinoi bezpeky v systemakh informatsiino-analitychnoho zabezpechennia pidtrymky pryiniattia orhanizatsiinykh rishen / Churubrova S. M. // Problemy prohramuvannia. 2016. № 4. S. 97-103.

5. Rozrobka polityky informatsiinoi bezpeky kompiuternoho kontroliu znan/ N. Kukharska// Visnyk Lvivskoho derzhavnoho universytetu bezpeky zhyttiediialnosti. 2017. №16. S.34-39.

6. Polityka informatsiinoi bezpeky obiekta/ Yu. Khokhlachova// Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini. 2012 r. Vyp. 2 (24). S. 23-29.

7. Otsiniuvannia efektyvnosti rishen v systemakh zakhystu informatsii/ V. Yu. Titova, O. S. Androshchuk, V. S. Orlenko, I. M. Shevchuk, V. S. Datsenko // Herald of Khmelnytskyi National University. Technical sciences. 2020. № 5. S. 307–310.

8. Komertsiina diialnist. Navch. posibnyk/ L.H. Fylevych, L.O. Popova, O.M. Priadko, T.L. Mitiaieva, L.A. Prybylovych. Kharkiv: KhDUKhT, 2014. 225 s.

9. Informatsiina polityka v systemi zabezpechennia finansovoi bezpeky derzhavy/ A.D. Hlushko, V.V. Pantas, S.R. Babenko// «Efektyvna ekonomika». 2022. №2.