JEL D80

МАРКУЦ Анастасія
аспірант, КНЕУ імені Вадима Гетьмана,
Україна,
ORCID: 0000-0001-7813-3733

e-mail: anastasiia.korzh@kneu.ua
Anastasia MARKUTS
PhD student,
KNEU named after Vadym Hetman,
Ukraine

КІБЕРЗАХИСТ ІНФОРМАЦІЇ НА АВТОНОМНОМУ ПІДПРИЄМСТВІ

Анотація: У публікації розглянуто особливості інформаційних технологій для захисту від кібератак на автономних підприємствах. Окрему увагу приділено кібербезпеці підприємств, і що це має бути пріоритетним напрямком на сучасних підприємствах.

Ключові слова: автономія підприємства, захист інформації, бізнес-економіка.

CYBER PROTECTION OF INFORMATION AT AN AUTONOMOUS ENTERPRISE

Abstract: The publication examines the features of information technologies for protection against cyber-attacks at autonomous enterprises. Particular attention is paid to the cyber security of enterprises, and that this should be a priority area in modern enterprises.

Keywords: autonomous enterprise, protection of information, economy of business.

Кібербезпека – це практика захисту комп'ютерів, серверів, мобільних пристроїв, електронних систем, мереж і даних від зловмисних атак. Вона також відома як безпека інформаційних технологій або електронна інформаційна безпека. Основні види захисту кібербезпеки:

— Безпека мережі – це практика захисту комп'ютерної мережі від зловмисників, будь-то цілеспрямовані зловмисники чи умовно-зловмисне програмне забезпечення.

— Безпека програм зосереджена на захисті програмного забезпечення та пристроїв від загроз. Зламана програма може надати доступ до даних, які вона призначена для захисту. Успішна безпека починається на етапі проектування, задовго до розгортання програми або пристрою.

— Інформаційна безпека захищає цілісність і конфіденційність даних, як під час зберігання, так і під час передачі.

— Операційна безпека включає процеси та рішення щодо обробки та захисту активів даних. Дозволи, які користувачі мають під час доступу до мережі, і процедури, що визначають, як і де дані можуть зберігатися або спільно використовуватися.

Аварійне відновлення та безперервність бізнесу визначають, як організація реагує на інцидент кібербезпеки або будь-яку іншу подію, що спричиняє втрату операцій або даних. Політика аварійного відновлення диктує, як організація відновлює свої операції та інформацію, щоб повернутися до тієї ж працездатності. Безперервність бізнесу – це план, до якого організація відступає, намагаючись працювати без певних ресурсів. Навчання кінцевих користувачів стосується найбільш непередбачуваного фактору кібербезпеки людей. Будь-хто може випадково занести вірус у захищену систему, не дотримуючись правил

безпеки. Навчання користувачів видаляти підозрілі вкладення електронної пошти, не підключати невідомі USB-накопичувачі та інші важливі уроки є життєво важливими для безпеки будь-якої організації[1,с.123-129].

Захист кінцевих користувачів або безпека кінцевої точки є важливим аспектом кібербезпеки. Зрештою, часто саме особа (кінцевий користувач) випадково завантажує шкідливе програмне забезпечення чи іншу форму кіберзагрози на свій настільний комп'ютер, ноутбук чи мобільний пристрій.

Отже, як методи кібербезпеки захищають користувачів та їхні дані від кібератаки? По-перше, кібербезпека покладається на криптографічні протоколи для шифрування електронних листів, файлів та інших важливих даних. Це не тільки захищає інформацію під час передачі, але й захищає від втрати чи крадіжки [3]. Крім того, програмне забезпечення безпеки кінцевих користувачів сканує комп'ютери на наявність частин шкідливого коду, поміщає цей код на карантин, а потім видаляє його з комп'ютера. Програми безпеки можуть навіть виявляти та видаляти шкідливий код, прихований у первинному завантажувальному записі, і призначені для шифрування або стирання даних з жорсткого диска комп'ютера. Захист інформації в кіберпросторі є неодмінною складовою економіки бізнесу.

Література

1.Коваленко, Ю. О. (2010). Забезпечення інформаційної безпеки на підприємстві. Економіка промисловості (3). с. 123–129.

2.Князев А. А. Информационная война Архівовано 26 березень 2014 у Wayback Machine. // Энциклопедический словарь СМИ. — Бишкек: Издательство КРСУ, 2002

3.Информационная безопасность (2-я книга социально-политического проекта «Актуальные проблемы безопасности социума»). М.: «Оружие и технологии», 2009.

References

1. Kovalenko, Y. O. (2010). Ensuring information security at the enterprise. Economy of industry (3). c. 123–129.

2. Knyazev A. A. Information war Archived 26 March 2014 at the Wayback Machine. // Encyclopedic Dictionary of Mass Media. - Bishkek: KRSU Publishing House, 2002

3. Information security (2nd book of the sociopolitical project "Actual problems of social security"). M.: "Arms and technologies", 2009.

JEL D80

ОБЕРЕМЧУК Валентина
к.е.н., доцент
КНЕУ імені Вадима Гетьмана, Україна,
ORCID: 0000-0001-9385-0714

ДЕМЧЕНКО Тарас
студент
Фаховий коледж інформаційних систем і технологій , КНЕУ імені Вадима Гетьмана, Україна,

e-mail: valentyna.oberemchuk@kneu.ua

Valentyna OBEREMCHUK
PhD, Associate Professor, KNEU named after Vadym Hetman, Ukraine; researcher, Otto-Friedrich-Universität Bamberg, Germany

Taras DEMCHENKO
student
Professional College of Information Systems and Technologies, KNEU named after Vadym Hetman