УДК 004.415.056:658.115

А. О. Азарова
В. Ф. Хісматулліна

ЕЛЕКТРОННІ ЗАСОБИ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ДЕРЖАВНИХ ПІДПРИЄМСТВАХ

Вінницький національний технічний університет

Анотація

В даній роботі досліджуються переваги та недоліки реалізації процесів захисту інформації на вітчизняних підприємствах на основі сучасних методів та засобів. Предметом дослідження є методи формування політики інформаційної безпеки на державних підприємствах.

Ключові слова: політика інформаційної безпеки, державне підприємство, інформаційна безпека, аутентифікація.

Abstract

In this work, the advantages and shortcomings of realizing information security processes at domestic state enterprises based on modern methods and tools are investigated. The subject of the research is the methods of formation of information security policy at state enterprises.

Key words: information security policy, state enterprise, information security, authentication.

Вступ

Із процесом розвитку активної інформатизації суспільства, який відбувається протягом кількох десятиліть в Україні і в усьому світі загалом, виникла нова глобальна проблема – інформаційна безпека. Також слід звернути увагу на те, що все більшого значення набуває забезпечення інформаційної безпеки на мікрорівні, а саме на рівні державних підприємств. Основні інтереси організацій в даний час значною мірою визначаються саме станом навколишнього інформаційного середовища. Цілеспрямовані або ненавмисні впливи на інформаційну сферу з боку зовнішніх або внутрішніх джерел можуть завдавати серйозної шкоди цим інтересам і становлять загрози та ризики для безпеки загалом. Сьогодні інформаційна безпека є необхідною та невід'ємною умовою для правильного і безперервного функціонування підприємства. Саме тому виникає необхідність розроблення і впровадження політики інформаційної безпеки на державних підприємствах.

Мета дослідження полягає у підвищенні рівня інформаційної безпеки на державних підприємствах засобами методів аутентифікації.

Результати дослідження

У процесі планування і проектування системи захисту інформації будь-якого державного підприємства, в першу чергу, необхідно розробляти та впроваджувати політику інформаційної безпеки. Політика безпеки – це набір законів, правил і практичних рекомендацій, на основі яких будується управління, захист і розподіл критичної інформації в системі [1]. Вона повинна охоплювати всі особливості процесу оброблення інформації конкретного підприємства, визначаючи при цьому поведінку системи в різних ситуаціях. Політика безпеки реалізується за допомогою організаційних заходів та програмно-технічних засобів, що визначають архітектуру системи захисту. Відсутність правильно розробленої та впровадженої політики інформаційної безпеки частіше за все стає причиною успішності зловмисників у випадках кібератак. Для конкретної організації політика безпеки повинна бути індивідуальною, залежною від конкретної технології оброблення інформації, використовуваних програмних і технічних засобів, розташування організації і т.п.

Якщо розглядати політику інформаційної безпеки з точки зору економічної безпеки підприємства, то все більш очевидною стає залежність загального рівня її від інформаційної складової. Практика показує, що будь-яка акція конкурентів, спрямована проти інтересів господарського суб'єкта, починається зі збору інформації: навіть дрібне розкрадання звичайно випереджає вивчення особою зі злочинними задумами можливості протиправних дій, і без відповідного інформаційного забезпечення

не представляються такі деструктивні прояви, як відведення активів підприємства або рейдерське захоплення [2-4].

Захист інформації, забезпечення інформаційної безпеки на підприємстві повинно носити системний характер, тобто різні засоби захисту (апаратні, програмні, фізичні, організаційні) повинні застосовуватися одночасно і під єдиним управлінням. Існує велика кількість інструментів забезпечення інформаційної безпеки: засоби ідентифікації та аутентифікації користувачів, засоби шифрування інформації, міжмережні екрани, віртуальні приватні мережі, засоби контентної фільтрації, інструменти перевірки цілісності вмісту дисків, засоби антивірусного захисту, системи виявлення вразливостей мереж і аналізатори мережевих атак. Як правило, кожен із цих інструментів має певні недоліки, крім того, під час розроблення політики інформаційної безпеки на підприємстві не можна нехтувати процедурою аутентифікації користувача – встановлення за допомогою спеціальних програмних засобів достовірності користувача [5].

Аутентифікація користувача включає дві процедури - ідентифікацію та верифікацію. Підсистема автентифікації користувачів – найважливіший компонент корпоративної системи інформаційної безпеки і її значення важко переоцінити [6]. Підсистема автентифікації підтверджує особу користувача інформаційної системи і тому повинна бути надійною і адекватною, тобто виключати всі помилки в наданні доступу. Майже всі методи аутентифікації страждають на один недолік - вони, насправді, аутентифікують не конкретного суб'єкта, а лише фіксують той факт, що аутентифікатор суб'єкта відповідає його ідентифікатору. Тобто всі відомі методи не захищені від компрометації аутентифікатора [7-10].

Отже, існуючі методи аутентифікації різні за ступенем надійності, і, як правило, з посиленням захисту різко зростає ціна систем, що вимагає при виборі засобів автентифікації аналізу ризиків та оцінки економічної доцільності застосування тих чи інших заходів захисту. Проте останнім часом «співвідношення сил» в області ефективності застосовуваних методів автентифікації змінюється. Саме тому, під час розроблення політики інформаційної безпеки конкретного підприємства важливо звернути увагу на те, якого виду засоби автентифікації будуть всебічно доцільними для використання.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2017. – 120 с.
2. Азарова А. О. Вибір, планування та реалізація стратегії розвитку підприємства [Текст] / А. О. Азарова, Н. С. Желюк // Актуальні проблеми економіки, №12. – 2010. – С. 91–100.
3. Азарова А. О. Розробка методики визначення економічної безпеки підприємства [Текст] / А. О. Азарова, О. В. Гаврилова // Збірник наукових праць «Економіка: проблеми теорії та практики». – Дніпропетровськ : ДНУ, 2004. – Вип.191, т. III. – С. 719–727.
4. Азарова А. О. Математичні моделі оцінювання стратегічного потенціалу підприємства та прийняття рішень щодо його підвищення [Текст] / А. О. Азарова, О. В. Антонюк. — Вінниця : ВНТУ, 2012. – 168 с.
5. Романец Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин ; под ред. В. Ф. Шаньгина. – 2-е изд., перераб. и доп. – М. : Радио и связь, 2001. – 376 с.
6. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа [Текст] / А.Ю. Щеглов. – СПб.: Наука и техника, 2004. – 384 с.
7. Свідоцтво про реєстрацію авторського права на твір №79708. Комп'ютерна програма „Захист інформації від несанкціонованого копіювання шляхом прив'язки до унікальних параметрів вінчестера і використання ключа активації" / Азарова А. О., Азарова Л. Є., Каплун І. С., Щербатюк А. В. Заявка від 05.06.2018 р. №80958. Дата реєстрації 11.06.2018 р.
8. Свідоцтво про реєстрацію авторського права на твір №79707. Розробка контролеру кодового доступу до сейфа на мікроконтролері Arduino / Азарова А. О., Азарова Л. Є., Каплун І. С., Щербатюк А. В. Заявка від 05.06.2018 р. №80960. Дата реєстрації 14.06.2018 р.
9. Свідоцтво про реєстрацію авторського права на твір №80464. Комп'ютерна програма „Мобільний додаток для захищеного передавання конфіденційних даних у смартфонах" / Азарова А. О., Азарова Л. Є., Бадя Ю. В. Заявка від 12.06.2018 р. №81238. Дата реєстрації 24.07.2018 р.
10. Свідоцтво про реєстрацію авторського права на твір №79708. Комп'ютерна програма „Програмний модуль ідентифікації користувача за відбитками пальців через смартфон з подальшою авторизацією" / Азарова А. О., Азарова Л. Є., Мисько Ю. О., Колган В. А. Заявка від 05.06.2018 р. №80951. Дата реєстрації 11.06.2018 р.

Азарова Анжеліка Олексіївна – к.т.н., проф. каф. МБІС, заст. декана Факультету менеджменту та інформаційної безпеки з наукової роботи та міжнародного співробітництва Вінницького національного технічного університету, м. Вінниця , e-mail: azarova.angelika@gmail.com.

Хісматулліна Валентина Фанілівна – студентка гр. УБ-15б факультету менеджменту та інформаційної безпеки, м. Вінниця, e-mail: khismatullinatina@gmail.com.

Azarova Anzhelika O. — Ph.D., Professor, Deputy dean of the Faculty of management and information security by scientific work and international cooperation Vinnytsia National Technical University, Vinnytsia.

Khismatullina Valentyna F. – Department of management and security of information systems, Vinnytsia National Technical University, Vinnytsia.