УДК 004.415.056:658.115

А. О. Азарова
Л. М. Ткачук
В. Ф. Хісматулліна

ФОРМУВАННЯ ЕФЕКТИВНОЇ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ПРОЦЕСАХ ПУБЛІЧНОГО УПРАВЛІННЯ

Вінницький національний технічний університет

Анотація

У даній роботі досліджуються методи реалізації процесів захисту інформації на підприємствах державного сегменту для ефективного їх функціонування та захисту. Предметом дослідження є методи формування політики інформаційної безпеки у процесах публічного управління.

Ключові слова: політика інформаційної безпеки, державний сегмент, інформаційна безпека, публічне управління.

Abstract

The methods of realizing information security processes at enterprises from state segment for those effective functioning and protection are investigated in this work. The subject of the research is the methods of information security policy formation in processes of public administration.

Key words: information security policy, state segment, information security, public administration.

Вступ

Із плином часу, все більшого значення набуває розроблення інформаційної безпеки підприємств державного сегменту у процесах публічного адміністрування. Складність розробки політики інформаційної безпеки визначається проблематичністю використання чужого досвіду, оскільки політика інформаційної безпеки ґрунтується на виробничих ресурсах і функціональних залежностях усередині об’єкта [1]. Необхідність формування політики інформаційної безпеки пояснюється необхідністю формування основ планування і управління інформаційною безпекою.

Мета розробки політики інформаційної безпеки – мінімізація ризиків бізнесу шляхом захисту інтересів об’єктів в інформаційній сфері, планування і підтримка безперервності функціонування, зниження витрат і підвищення ефективності інвестицій в захист інформації.

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 [2]. 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.

Концепція побудови системи інформаційної безпеки повинна будуватися на принципах, характерних для системи безпеки підприємства, тобто кожен працівник повинен себе ідентифікувати при вході в систему, по аналогії з записом в журналі відвідувань, присвоювати різні ступені доступу інформації (такі як інформація з обмеженим доступом, чи конфіденційна інформація) аналогічно забороні доступу до певних приміщень, повинна бути заборона вчиняти певні дії та багато іншого [3]. Необхідно пам’ятати, що в більшості випадків пересічний користувач не зрозуміє реальних ризиків

від вчинених ним дій, навіть якщо чітко пояснити, що просте відкриття листа з невідомої електронної пошти може призвести до зламу всієї мережі підприємства [4].

Також потрібно пам'ятати, що Політика ІБ – це лише загальний документ (свого роду Конституція інформаційної безпеки), загалом же Інформаційна безпека повинна поділятися на рівні: Політика Інформаційної безпеки; спеціалізовані документи з різних напрямків інформаційної безпеки (Політика конфіденційності, Політика реагування на кіберінциденти); вузькопрофільні документи, які регулюють вчинення конкретних дій працівниками в рамках Політики інформаційної безпеки (процедури, регламенти, посадові інструкції осіб відповідальних за інформаційну безпеку) [5].

На сьогодні в Україні немає чітко врегулювання вимог до Інформаційної безпеки на підприємствах. При цьому є вимоги які ставляться до компаній, які працюють з персональними даними громадян Європейського союзу відповідно до вимог General data protection regulation (GDPR), та деяких інших нормативних актів. Останні тенденції нормотворення, зокрема, проект Постанови НБУ «Про затвердження Положення про кіберзахист та інформаційну безпеку в платіжних системах та системах розрахунків», окремі норми Закону України «Про основні засади забезпечення кібербезпеки України» та деякі інші, вказують на те, що в близькому майбутньому нас чекає чітке законодавче регулювання з жорсткими вимогами до Політик інформаційної безпеки підприємств державного сегменту [6-12].

Висновки

Для забезпечення достатнього рівня інформаційної безпеки у процесах публічного адміністрування потрібно розробляти політику інформаційної безпеки з урахуванням того, що вона є складовою системи безпеки підприємства, і пам'ятати, що вона повинна бути орієнтованою на кожного працівника, а також не навантажувати головний документ інформацією, направленою на окремих працівників. Для цього потрібно розробляти документи нижчого рівня.

Якщо ж говорити про те, технічний це чи юридичний документ, потрібно поєднати технічне знання з юридичними вміннями по написанню зрозумілих для кінцевого користувача документів подібних по своїй формі, швидше до user friendly керівництв, ніж до технічних посібників.

При розробці політики інформаційної безпеки та інших документів для забезпечення кібербезпеки у процесах публічного адміністрування, ми виходимо з необхідності встановлення захисту системи від зовнішніх та внутрішніх атак та гнучкості, важливої для розуміння документів працівниками.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Голубенко О. Л. Політика інформаційної безпеки / Голубенко О. Л., Хорошко В. О., Петров О. С., Головань С. М., Яремчук Ю. Є. – Луганськ: Вид. СНУ ім. В. Даля, 2009. – 300 с.
2. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2017. – 120 с.
3. Ленков С. В. Методы и средства защиты информации. В 2-х томах / Ленков С. В., Перегудов Д. А., Хорошко В. А. – К.: Арий, 2008.
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. 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.
7. 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.
8. 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.
9. 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.
10. Азарова А. О., Гудзь В. О., Блонський В. О. Управління інформаційною безпекою в державних установах на основі біометричної аутентифікації відбитків пальців для захисту інформації від несанкціонованого доступу. Тези XLVIII науково-технічної конференції ВНТУ. 2019. URL: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2019/paper/view/7429 (дата звернення: 22.04.2019).
11. Азарова А. О., Гудзь В. О., Блонський В. О. Управління та адміністрування захистом інформації шляхом локалізації закладних пристроїв на основі індитикатора електромагнітних випромінювань. Тези XLVIII науково-технічної конференції ВНТУ. 2019. URL: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2019/paper/view/7335/6122 (дата звернення: 22.04.2019).

12. Азарова А. О., Хісматулліна В. Ф. Електронні засоби політики інформаційної безпеки на державних підприємствах. Тези XLVIII науково-технічної конференції ВНТУ. 2019. URL: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2019/paper/view/6889 (дата звернення: 22.04.2019).

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.

Ткачук Людмила Миколаївна – к.е.н., доц. каф. МБІС, заст. декана Факультету менеджменту та інформаційної безпеки з навчально-методичної роботи Вінницького національного технічного університету, м. Вінниця, e-mail: ludatkachuk2017@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.

Lyudmila Tkachuk – PhD (Ec), Assistant Professor, Deputy dean of the Faculty of management and information security by educational work of Vinnytsia National Technical University, Vinnitsa, email : ludatkachuk2017@gmail.com

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