Секція: Економічна безпека

РУСІНА ЮЛІЯ ОЛЕКСАНДРІВНА
кандидат економічних наук
доцент кафедри фінансів та фінансово-економічної безпеки
Київський національний університет технологій та дизайну
ОСТРЯКОВА ВАЛЕНТИНА ЮРІЇВНА
студентка кафедри фінансів та фінансово-економічної безпеки
Київський національний університет технологій та дизайну

УДОСКОНАЛЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

В умовах сучасної економіки інформація стосовно всіх напрямків діяльності підприємства є найбільш цінним ресурсом, а проблеми інформаційної безпеки – усе складнішими і значущими. Інформаційна безпека є однією зі складових частин економічної безпеки, яка формує систему захищеності підприємства.

Дослідженню питання забезпечення інформаційної безпеки присвячено праці С. Арзуманова, С. Кавуна, І. Конєєва, О. Тарасової, В. Домарєва, Є. Степанова, С. Петренка, О. Юдіна та ін.

Згідно з міжнародним стандартом ISO/IEC 27001:2005, система управління інформаційною безпекою – це «частина загальної системи управління, яка ґрунтується на підході, що враховує бізнес-ризики, призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки» [1]. Її основними цілями є: конфіденційність інформації; неможливість несанкціонованого доступу до інформації; цілісність інформації, та пов'язаних з нею процесів; доступність інформації; мінімізація ризиків інформаційної безпеки шляхом виконання компенсаційних заходів; облік

усіх процесів, пов'язаних з ризиками.

На практиці інформаційна безпека підприємства включає сукупність методів, напрямів, засобів і заходів, що знижують вразливість інформації і перешкоджають несанкціонованому доступу до інформації, її розголошенню або витоку. Елементами цієї системи є: правовий, організаційний, інженерно-технічний захисти інформації, а основною її характеристикою – комплексність [2]. Структура системи, зміст і склад елементів, їх взаємозв'язок залежать від обсягу і цінності інформації, що захищається, характеру можливих загроз безпеки інформації, необхідної надійності захисту і вартості системи.

Дослідивши та проаналізувавши публікації М. Журавля, С. Кавуна, І. Конєєва та О. Тарасової [3; 4; 5; 6], можна зазначити, що інформаційній безпеці в сучасних умовах було приділено недостатньо уваги. Про це свідчать важливі недоліки відповідно до забезпечення інформаційної безпеки підприємств:

- відсутність паролів доступу в систему;
- відсутність паролів при роботі програмою з 1С: Підприємство, при зміні даних;
- відсутній додатковий захист файлів та інформації;
- нерегулярне оновлення баз програми антивіруса і сканування робочих станцій;
- велика кількість документів на паперових носіях, в основному, лежать в папках на робочому столі співробітника, що дозволяє зловмисникам скористатися даного роду інформацією у власних цілях;
- не проводиться регулярне обговорення питань інформаційної безпеки на підприємстві і виникаючих проблем у цій галузі;
- не організована регулярна перевірка працездатності інформаційних систем підприємства, налагодження проводиться тільки лише в тому випадку, коли вони виходять з ладу;

- відсутня політика інформаційної безпеки;
- відсутність системного адміністратора.

Для виконання поставлених цілей і вирішення завдань необхідно провести заходи на всіх рівнях інформаційної безпеки (рис. 1).

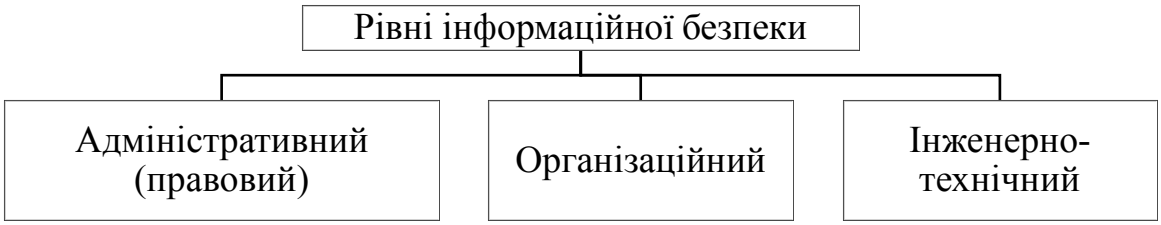

Рис. 1. Рівні інформаційної безпеки (складено автором на основі джерела [7])

На адміністративному (правовому) рівні для формування системи інформаційної безпеки необхідно розробити та затвердити політику інформаційної безпеки.

Політика безпеки – це сукупність документованих управлінських рішень, спрямованих на захист інформації та асоційованих з нею ресурсів [8].

Залежно від сформульованої політики, можна вибирати конкретні механізми, що забезпечують безпеку системи.

На організаційному рівні необхідно застосувати наступні заходи щодо поліпшення захисту інформації:

- організація робіт з навчання персоналу навичкам роботи з новими програмними продуктами за участі кваліфікованих фахівців;
- розробка заходів, спрямованих на вдосконалення системи економічної, соціальної та інформаційної безпеки підприємства.
- проведення інструктажу для того, щоб кожен співробітник усвідомив всю важливість і конфіденційність, довіреної йому, інформації;
- контроль за дотриманням співробітниками правил роботи з конфіденційною інформацією;

- планове проведення зборів, семінарів, обговорень з питань інформаційної безпеки підприємства;
- регулярна перевірка і обслуговування всіх інформаційних систем та інформаційної інфраструктури на працездатність.

Інженерно-технічний рівень передбачає застосування наступних заходів:

- введення паролів користувачів;
- розмежування доступу до файлів, каталогів, дисків (здійснюється системним адміністратором, який дозволяє доступ до відповідних дисків, папок і файлів для кожного користувача конкретно);
- регулярне сканування робочих станцій і оновлення баз антивірусної програми;
- застосування джерел безперебійного живлення;
- криптографічне перетворення інформації (криптографічний захист інформації надається з метою забезпечення режиму конфіденційності та цілісності інформації при її передачі по каналах передачі даних).

Ефективність системи інформаційної безпеки і праці адміністраторів, засобів інформаційної безпеки буде неефективною за відсутності засобів збору, аналізу, зберігання інформації про стан системи, централізованого управління всіма її складовими. Адже, кожен засіб захисту реалізує певну складову політики безпеки, яка на рівні підсистем задається набором параметрів і вимог. Політиці інформаційної безпеки повинні відповідати не тільки кожна підсистема або засіб захисту, але й система в цілому.

Реалізація заходів щодо удосконалення системи інформаційної безпеки на підприємствах дозволить: розмежувати права доступу в систему; підвищити рівень захищеності інформації кожного користувача окремо, і системи в цілому; розробити та впровадити політику інформаційної безпеки, яка буде спрямована на захист інформації та

асоційованих з нею ресурсів; зменшити кількість спаму; відображати шкідливі атаки через мережу; підвищити рівень захисту робочих станцій.

Література:

1. ISO/IEC 27001:2005, MOD. – [Електронний ресурс]. – Режим доступу: http://s-byte.com/useful/27001.pdf
2. Аникин И.В. Теория информационной безопасности и методология защиты информации [Текст] /И.В. Аникин, В.И. Глова, Л.И. Нейман, А.Н. Нигматуллина . — Казань : Изд-во Казан. гос. техн. ун-та, 2008. — 358с.
3. Журавель М. М. Проблеми захисту інформації [Електронний ресурс] / М. М. Журавель, С. В. Паршуков. – Режим доступу: http://informatika.udpu.org.ua/?page_id=1173
4. Кавун С. В. Інформаційна безпека. Навчальний посібник. Ч.1 / С. В. Кавун, В. В. Носов, О. В. Мажай. – Харків : Вид. ХНЕУ, 2008. – 352 с.
5. Конеев И. Р. Информационная безопасность предприятия / И. Р. Конеев, А. В. Беляев. – СПб. : БХВ-Петербург, 2003. – 747 с.
6. Тарасова О. В. Корпоративна культура як інструмент ефективного менеджменту підприємства. / О. В. Тарасова, С. С. Марінова // Економіка харчової промисловості. – 2013. – № 3(19). – С. 28–32.
7. Донець Л.І., Ващенко Н.В. Економічна безпека підприємства: Навч. пос. - К.: Центр учбової літератури, 2008. - 240 с.
8. Романова Ю. Д. Інформаційні технології в менеджменті (управлінні): підручник і практикум для академічного бакалаврату / під заг. ред. Д. Ю. Романової. – М: Видавництво Юрайт, 2015. – 478 с.