УДК 338.432

О.М. Лобода, В.С. Фесенець
Херсонський державний аграрно-економічний університет
Len.loboda@ukr.net

ЗАСТОСУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ПІДПРИЄМСТВА

У сучасних умовах інформаційні ресурси є незамінними для розвитку науки, техніки, виробництва, послуг та інших складових промисловості. Виникає проблема класифікації інформаційних ресурсів, обмеження доступу до деяких із них та визначення економічної доцільності організації захисту інформації на підприємствах та в організаціях різних сфер економічної діяльності. Інформаційна безпека з погляду економічної безпеки – це стан захищеності діяльності організації та її інформаційного середовища від негативного впливу факторів, що дестабілізують, що забезпечує збереження основних властивостей інформації та досягнення соціально-економічної мети.

Інформаційна загроза виникає, коли величина та ймовірність потенційної інформаційної шкоди перевищує певний поріг, що вимагає комплексу заходів щодо її запобігання та захисту об’єкта безпеки. Загрози інформаційній безпеці – це події або дії, які можуть призвести до спотворення, несанкціонованого використання або навіть знищення інформаційних ресурсів системи управління, апаратного та програмного забезпечення [1, с.21].

Загроза збереження цілісності та конфіденційності інформаційних ресурсів з обмеженим доступом практично реалізована, оскільки існує ризик створення каналу несанкціонованого отримання цінної інформації та документів. Функціонування каналу несанкціонованого доступу до інформації неминуче призводить до втрати інформації, зникнення носія інформації. Забезпечення інформаційної безпеки слід починати з визначення питань взаємовідносин, пов'язаних з використанням інформаційних систем. Їх інтереси можна розділити на такі категорії: доступність, цілісність і конфіденційність [2, с.153].

Тобто у найзагальнішому вигляді інформаційну безпеку можна визначити як неможливість компрометації властивостей об'єкта безпеки, що визначаються інформацією та інформаційною інфраструктурою. До об'єктів забезпечення інформаційної безпеки в організації належать: інформаційні ресурси, що містять відомості, що належать до комерційної таємниці та конфіденційної інформації, подані у вигляді інформаційних масивів та баз даних; інформаційні засоби та системи; комп'ютерне та організаційне обладнання; мережі та системи; загальне системне та прикладне програмне забезпечення; автоматизовані системи управління в організаціях; системи зв'язку та передачі даних; технічні засоби збирання; Реєстрація, передача, обробка та відображення інформації [3, с.61]. До основних загроз безпеці відносяться: розкриття конфіденційної інформації; несанкціоноване використання інформаційних ресурсів; нецільове використання ресурсів; несанкціонований обмін інформацією; злом системи; дискредитувати.

До причин і умов, що створюють умови для втрати інформації, належать: недостатня поінформованість працівників організації про правила захисту конфіденційної інформації та нерозуміння необхідності їх ретельного дотримання; використання несертифікованих технічних засобів для обробки конфіденційної інформації; слабкий контроль за дотриманням правил захисту інформації за допомогою правових, організаційних та технічних заходів і т.д.; обробка та передавання даних.

У цілому нині система управління діяльністю підприємства мало чим відрізняється від системи управління виробництвом товарної продукції, хоча має свої особливості. Однак при розробці системи надання послуг, а отже, і системи управління необхідно враховувати такі фактори: місцезнаходження обслуговуючого підприємства насамперед визначається місцезнаходженням споживачів; потреби та бажання споживачів. Графік роботи переважно залежить від споживачів; важко визначити та виміряти якість. Співробітники повинні мати добрі навички спілкування зі споживачами. Виробнича потужність зазвичай розраховується з

урахуванням пікового споживчого попиту, а чи не середнього попиту. продуктивність праці може бути обумовлена відсутністю споживчого попиту, а не низькою продуктивністю праці. Великі компанії у сфері послуг не характерні (винятки становлять авіакомпанії, банки); Маркетингові та виробничі послуги іноді важко поділити. Слід наголосити на винятковій динаміці сервісної діяльності, яка демонструє яскраво виражену тенденцію до індивідуалізації потреб клієнтів. При цьому існує закономірність: чим вищий рівень життя населення, чим більшою кількістю послуг люди можуть скористатися, тим нетиповішими й унікальнішими стають їхні запити. У відповідь на цю тенденцію, а також посилення конкуренції у цій сфері, сервісні організації змушені постійно розширювати спектр послуг та підвищувати їхню якість, прогнозувати і навіть проектувати попит. Проте така інноваційна діяльність завжди супроводжується обмеженими ресурсами: фінансовими, людськими, матеріальними.

З погляду системного підходу до забезпечення інформаційної безпеки встановлюються певні умови: забезпечення інформаційної безпеки може бути разовим; це безперервний процес, що полягає в обґрунтуванні та впровадженні найбільш раціональних методів, засобів та способів удосконалення та розвитку системи захисту, постійному контролі за її станом, виявленні вузьких та вразливих місць та протиправних дій; планування інформаційної безпеки здійснюється шляхом розробки докладних планів безпеки у сфері відповідальності кожним агентством.

Інформаційна безпека вимагає конкретних даних, які мають бути об'єктивно захищені та втрата яких може призвести до значних втрат для організації. Методи та засоби захисту повинні надійно блокувати можливі шляхи несанкціонованого доступу; ефективність захисту інформації означає, що вартість її реалізації не повинна перевищувати можливі втрати від реалізації інформаційних загроз; чітко визначені повноваження та права користувача щодо доступу до певних видів інформації; надання користувачеві мінімальних повноважень, необхідні виконання дорученої роботи; зведення до мінімуму кількості захистів, які спільно використовуються кількома користувачами. Фіксація випадків несанкціонованого доступу до конфіденційної інформації; забезпечення рівня конфіденційності інформації; Забезпечення контролю цілісності засобів захисту та негайне реагування на будь-який збій.

Тому система захисту має мати певні види власного забезпечення: юридичне забезпечення, тобто нормативні документи, положення, інструкції; організаційне забезпечення, тобто здійснення захисту інформації, яке здійснюється окремими структурними підрозділами, тобто службою безпеки, службою безпеки, службою захисту інформації, технічними засобами тощо, апаратне забезпечення, інформаційна підтримка, програмне забезпечення; математичне програмне забезпечення; нормативно-методичне та ергономічне забезпечення. Тому зміст компонентів елементів, методів та засобів захисту інформаційних ресурсів у межах будь-якої системи захисту має постійно змінюватися з метою запобігання їх розголошенню суб'єктом даних.

ЛІТЕРАТУРА:

1. Кузнецов О. О. Захист інформації в інформаційних системах: навч. посіб. Х.: ХНЕУ, 2018. 510 с.
2. Лобода О.М., Кириченко Н.В. Базові комунікаційні технології: навч. посіб. Херсон: Стар, 2018. 235 с.
3. Лобода О.М. Захист інформації в корпоративних мережах. *Публічне управління та адміністрування у процесах економічних реформ*: матеріали IV Всеукр. наук.-практ.конф., м. Херсон, 11 лист. 2020р. ХДАЕУ, 2020. С.61-63.
4. Марасанов В.В., Пляшкевич О.М. Основи теорії проектування і оптимізації макроекономічних систем. Херсон: Айлант, 2002.190с.
5. Лобода О.М., Кириченко Н.В. Актуальні проблеми ідентифікації та моделювання структури управління підприємством. *Наука й економіка*, 2015. №3. С.130-134.