*України У 2 томах / А. Й.Рогожин, М. М. Страхов, В. Д. Гончаренко та т - К Ін Юре, 1996. **10.** Історія держави і права України – Підручник У 2-х т. / За ред. В. Я. Тація, А. Й. Рогожина, В. Д. Гончаренка -Том 1 - Кол авторів В. Д. Гончаренко, А Й Рогожин, О. Д. Святоцький та ін.- К Концерн "Видавничий дім "Ін Юре", 2003 - 656 с. **11.** Хавронюк М. І. Військові злочини Навчальний посібник Академія внутрішніх справ МВС України , Київ 1995 р. **12.** Слабченко М. Е. Опити по истории права Малороссии XVII - XVIII ст -Одеса, 1911; **13.** Грозовський І. М. Козацьке правоі / Право України -1997 р. - №6; **14.** Развитие русского права в XV - первой половине XVII в. - М Юрид литература 1986 р. **15.** Владимирский-Буданов М. Ф. Отношения между Литовским статутом и Уложением царя Алексея Михайловича // Сборник государственних знаний -Т IV - СПб, 1877 р. **16.** Тельберг Г. Г. Система государственных преступлений в уложении царя Алексея Михайловича // Журнал Министерства Юстиции, №5, 6 – 191; 1 **17.** Соборное уложение 1649 года. Текст Комментарии /Подред А. Г. Манькова - Л Наука 1987; **18.** Законодательство Петра І Клеандрова В. М., Колобов Б. В., Кутьина Г. А., и др., оте ред. Преображенский А. А. и Новицкая Т. Е., – М Юридическая литература, 1997 р. **19.** Ромашкин П. С. Основниие начала уголовного и военно-уголовного законодательства Петра І – М, 1947 р. **20.** Історія держави і права У країни Частина 1 [Підруч. Для юрид вищих навч закладів і фак / А. Й. Рогожин, М. М. Страхов, В. Д. Гончаренко та ін.] За ред. Акад. Академії правових наук України А. Й. Рогожина – Х Основа, 1993р. – 432 с. **21**. Права за якими судиться малоросійський народ 1743 / Під редакцією Ю. С. Шемшученка Наукове видання –К. АТ "Книга", 1997 р.*

УДК 638.235.231

ЦИКЛ ВПРОВАДЖЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Віталій Безштанько
Спеціальний факультет СБ України ВІТІ НТУУ "КПІ"

Анотація: **Розглядається цикл впровадження системи управління інформаційною безпекою відповідно до ISO/IEC 27001:2005(E).**
Summary: **The cycle of introduction of the Information Security Management System is examined, in accordance with ISO/IEC 27001:2005(E).**
Ключові слова: **Цикл, система, управління, інформація, безпека.**

I Вступ

У результаті інтенсивного використання інформаційних технологій практично в усіх сферах діяльності задачі управління сучасною організацією та її інформаційною безпекою з кожним днем стають все складнішими. Все частіше перед спеціалістами інформаційної безпеки ставиться задача не просто впровадити засоби або систему захисту, а й побудувати систему управління інформаційною безпекою.

Правильна побудова, впровадження, функціонування, контроль, вчасне коригування, підтримка і поліпшення системи управління інформаційною безпекою (далі - СУІБ) є важливою задачею керівника, який прагне створити конкурентноспроможну, прибуткову, що відповідає законодавству та комерційній репутації, організацію. Для ефективного функціонування СУІБ організації важливим є:

а) розуміння вимог, необхідності впровадження політики та цілей інформаційної безпеки;

б) впровадження та функціонування важелів контролю з метою управління ризиками інформаційної безпеки;

в) контроль і коректування ефективності роботи СУІБ, її безперервне вдосконалення, засноване на об'єктивній оцінці ризиків.

Для впровадження принципів управління ризиками, схемою безпеки і коректуванням СУІБ доцільно використовувати цикл "Планування - дія - перевірка - функціонування".

II Планування

На етапі планування організація повинна:

1. залежно від характеру діяльності організації, її місця розташування, ресурсів та технологій, що використовуються, визначити масштаб та межі СУІБ;

2. визначити, схвалити та затвердити керівництвом політику СУІБ залежно від характеру діяльності організації, її ресурсів та технологій, що вживаються, яка:

- включає визначення інформаційної безпеки, наміри керівництва з управління інформаційною безпекою, короткий опис політики безпеки, принципів та стандартів, які мають значення для організації;
- визначає загальні та приватні обов'язки з управління інформаційною безпекою, а також надає відомості про інциденти;
- включає посилання на документацію, яка може доповнювати опис політики, наприклад, більш докладний опис політик та інструкцій для конкретних інформаційних систем або правила безпеки, яких повинен дотримуватися користувач;
- включає схему постановки цілей і встановлює загальний напрямок та принципи діяльності, що стосуються захисту інформації;
- приймає до уваги ділові та нормативні вимоги, а також контрактні зобов'язання, в яких фігурують питання безпеки;
- направляє стратегію управління ризиками організації, в якій планується побудувати та підтримувати СУІБ;
- встановлює критерії, за якими буде проводиться оцінка ризиків;

3. визначити:
- методи оцінки ризиків, які відповідають СУІБ, нормативним, діловим, а також із забезпечення інформаційної безпеки вимогам;
- критерії для прийняття ризиків та їх допустимі рівні;

4. для описання ризиків визначити:
- інформаційні ресурси організації та їхніх власників;
- загрози цим ресурсам;
- вразливості;
- рівень збитку при можливому порушенні конфіденційності, цілісності або доступності інформаційних ресурсів;
- вірогідність такого порушення з урахуванням відомих небезпек, вразливостей та реалізованих засобів захисту;

5. проаналізувати та оцінити:
- ризики ділових невдач організації, які можливо відбулися б через втрату конфіденційності, цілісності або доступності інформаційних ресурсів;
- реальну вірогідність порушення безпеки та збитки організації у випадку реалізації загрози, а також визначити методи контролю, які використовуються в даний момент;
- чи потребують прийняті ризики застосування додаткових заходів для їхнього пониження;

6. оцінити методи усунення ризиків, для чого потрібно:
- визначити відповіді методи контролю;
- свідомо і об'єктивно прийняти ризик, що відповідає визначеному політикою безпеки організації рівню;
- визначити шляхи уникнення ризиків;

7. визначити цілі та методи перевірок результатів усунення ризиків, які повинні відповідати вимогам:
- нормативним;
- договірним;
- прийняття ризиків в організації;

8. отримати дозвіл керівництва на запропоновані рівні ризиків, що залишились;
9. отримати повноваження керівництва на впровадження та роботу СУІБ.

III Дія (впровадження та функціонування СУІБ)

На цьому етапі організація повинна:

1. сформувати план усунення ризику, який визначає:
- необхідні дії з управління;
- відповідальність за його виконання;
- інформаційні ресурси організації;
- пріоритети управління ризиками інформаційної безпеки;

2. впровадити план усунення ризиків;
3. впровадити заходи, визначені на етапі планування;
4. визначити методику оцінки керівництвом ефективності досягнення запланованих заходів безпеки;

5. впровадити програми ознайомлення та навчання заходам безпеки для того, щоб гарантувати, що весь персонал, який несе відповідальність за СУІБ, достатньо компетентний для виконання необхідних задач;
6. документувати записи про освіту, навчання, навики, досвід та кваліфікацію персоналу;
7. визначити та надати ресурси, необхідні для:

– впровадження, функціонування, моніторингу, коректування, підтримки та удосконалення СУІБ;
– того, щоб гарантувати, що заходи інформаційної безпеки не суперечать бізнес вимогам;
– приведення до відповідності нормативних вимог та договірних обов'язків безпеки;
– підтримки достатнього рівня безпеки за допомогою правильного використання всіх впроваджених заходів;
– в разі необхідності, коректування СУІБ;
– покращення ефективності роботи СУІБ.

IV Перевірка (перевірка та коректування СУІБ)

На цьому етапі організація повинна:

1. здійснювати заходи перевірки та коректування СУІБ для того, щоб:

– швидко знаходити помилки в результатах обробки даних;
– оперативно визначати успішні та неуспішні спроби порушення інформаційної безпеки;
– надати керівництву можливість оцінити успішність функціонування в організації системи забезпечення безпеки, що була делегована співробітникам та реалізована технічними засобами;
– запобігати спробам порушення інформаційної безпеки;
– визначати ефективність впроваджених заходів усунення порушень безпеки;

2 на основі результатів перевірок безпеки та подій, що трапилися, здійснювати регулярні заходи з підвищення ефективності СУІБ;

3. оцінювати ефективність заходів контролю для того, щоб впевнитись у виконанні вимог безпеки;

4. коригувати методику оцінки ризиків через заплановані проміжки часу, беручи до уваги зміни, що трапились в:

– організації;
– технології;
– ділових задачах і процесах;
– визначених загрозах;
– оцінці результатів впроваджених заходів безпеки;
– зовнішніх подіях, таких, як зміни в нормативно-правових документах, контрактних зобов'язаннях та соціальній сфері;

5. проводити внутрішні перевірки СУІБ через заплановані проміжки часу для того, щоб визначити, що заходи забезпечення безпеки та контролю:

– відповідають вимогам нормативно-правових документів та контрактним зобов'язанням;
– відповідають визначеним вимогам інформаційної безпеки організації;
– ефективно впроваджуються;
– працюють як очікувалося;
– зберегли свою ефективність.

Внутрішні перевірки СУІБ мають враховувати результати попередніх перевірок. Потрібно визначити їхні критерії оцінки, масштаби, періодичність та методики, що будуть застосовуватися. Вибір аудиторів та методів перевірок має гарантувати об'єктивність та неупередженість їх проведення. Аудитори не можуть перевіряти свою роботу. Відповідальність, планування та проведення перевірок, надання їхніх результатів, мають бути задокументовані. Документи, що відображають результати перевірок, необхідно захищати та контролювати, а керівництву, відповідальному за перевірки, – гарантувати, що дії з усунення виявлених помилок та їхніх причин застосовуються негайно. Подальші дії мають включати перевірку впроваджених заходів та повідомлення про її результати.

6. на цьому етапі організація повинна з визначеною періодичністю (як мінімум один раз на рік) проводити коректування СУІБ для того, щоб гарантувати її необхідність, ефективність та актуальність. Коректування мають включати оцінку можливості удосконалення та необхідності внесення змін до СУІБ, політики, задач інформаційної безпеки. Результати коректування СУІБ необхідно задокументувати. При цьому вести записи дій та подій, які можуть мати вплив на ефективність роботи СУІБ.

V Функціонування (підтримка і удосконалення СУІБ)

Під час функціонування СУІБ організація повинна:

1. постійно здійснювати удосконалення СУІБ з використанням вимог політики інформаційної безпеки та результатів:
   - перевірок СУІБ;
   - аналізу подій;
   - коректування керівництвом;
2. здійснювати необхідні заходи для усунення причин виникнення невідповідності вимогам СУІБ з метою запобігання їх повторній появі;
3. визначити необхідні попереджувальні дії для усунення можливих невідповідностей вимогам СУІБ та запобіганню їх появі; попереджувальні дії, що застосовуються, мають відповідати можливій проблемі;
4. визначити ризики, що змінилися, та необхідність попереджувальних заходів; пріоритети попереджувальних заходів мають бути визначені на підставі результатів оцінки ризиків;
5. застосовувати досвід, отриманий внаслідок порушення безпеки в інших організаціях та в своїй безпосередньо;
6. повідомляти про дії та удосконалення СУІБ всім зацікавленим сторонам з рівнем деталізації, залежно від обставин;
7. гарантувати, що вдосконалення досягли поставлених цілей.

Отже, використання циклу впровадження СУІБ відповідно до міжнародного стандарту ISO/IEC 27001:2005(E) значно підвищить рівень забезпечення та контролю за інформаційною безпекою в організації, а також дасть змогу керівнику створити конкурентноспроможну, прибуткову, таку, що відповідає законодавству та комерційній репутації організацію.

*Література:**1**. Information technology — Security techniques — Information security management systems — Requirements ISO/IEC 27001:2005(E),* ***2.*** *Information technology — Code of practice for information security management. First edition 2000-12-01 ISO/IEC 17799:2000(E).*

УДК 638.235.231.

АН АЛІЗ ЗАКОНОДАВСТВА В ГАЛУЗІ ЗАХИСТУ ІНФОРМАЦІЇ

Василь Цуркан

Спеціальний факультет СБ України ВІТІ НУТУ «КПІ»

Анотація: **На основі аналізу чинного законодавства визначено підхід до забезпечення захисту інформації в автоматизованих системах.**

Summary: **On the Basis of analysis of current legislation, approach was certain to providing of defence of information in the automated systems.**

Ключові слова: **Захист інформації, комплексна система захисту інформації, автоматизована система, несанкціонований доступ, обчислювальна система, захист від несанкціонованого доступу, комплекс засобів захисту, атрибути доступу, довірче та адміністративне керування доступом, критерії оцінки захищеності інформації.**

Відповідно до НД ТЗІ 1. 1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» захисту від різноманітних за своєю сутністю впливів вимагають інформаційні ресурси держави або суспільства в цілому, а також окремих організацій та фізичних осіб, які являють собою цінність, мають відповідне матеріальне вираження. Захистити інформацію – означає створити та підтримувати в дієздатному стані систему заходів, які дозволяють запобігти або ускладнити можливості реалізації різноманітного роду загроз відносно автоматизованої системи, а також знизити потенційні збитки від їх впливу. Система зазначених заходів, що забезпечує захист інформації, називається комплексною системою захисту інформації[1, 2].

Автоматизована система [1] являє собою організаційно-технічну систему, що реалізує інформаційну технологію і об'єднує обчислювальну систему (сукупність програмно-апаратних засобів, призначених для обробки інформації), фізичне середовище, персонал і інформацію, що обробляється. Виділяють три ієрархічні класи автоматизованих систем [3]. Це дозволяє, по-перше, врахувати особливості функціонування кожного з них при розробці профілів захищеності інформації, яка обробляється, а, по-