УДК 519.711

М.Ю. Комаров, Київ
С.Ф. Гончар, Київ

МЕТОДИКА ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Abstract. A review of the standards of the ISO 2700x series. The basic principles and methods of building a system for information security are considered.

Актуальність

Безперервний розвиток інформаційних технологій, а також обрана Україною стратегія інтеграції до міжнародних політичних та економічних інституцій, вимагає всебічної та чіткої гармонізації національних стандартів України в галузі інформаційної безпеки з відповідними міжнародними стандартами, зокрема стандартами серії ISO 2700x [1- 6].

Побудова та впровадження систем управління інформаційною безпекою (СУІБ) в установах та організаціях енергетичного сектору всіх форм власності, в яких передбачається обробка інформації з обмеженим доступом (конфіденційна, службова, інформація, що становить державну таємницю), а також на об'єктах критичної інфраструктури є актуальною задачею в контексті забезпечення комплексного підходу захищеності інформаційних ресурсів, які на них розміщені.

Постановка задачі

Необхідно вирішити наступні задачі:

- здійснити аналіз методів та принципів побудови СУІБ з метою можливості їх впровадження в установах та організаціях енергетичного сектору та на об'єктах критичної інфраструктури;
- визначити можливість інтеграції СУІБ до існуючих комплексних систем захисту інформації, що побудовані на об'єктах інформаційної діяльності, або можливість їх безконфліктної гармонізації.

Вирішення задачі

Управління інформаційною безпекою – це циклічний процес, що включає усвідомлення ступеня необхідності захисту інформації та постановку завдань; збір та аналіз даних про стан інформаційної безпеки в організації; оцінку інформаційних ризиків; планування заходів з обробки ризиків; реалізацію та впровадження відповідних механізмів контролю, розподіл ролей і відповідальності, навчання і мотивацію персоналу, оперативну роботу із здійснення заходів захисту; моніторинг функціонування механізмів контролю, оцінку їх ефективності та відповідні коригувальні дії.

Згідно ISO 27001 [2], система управління інформаційною безпекою (СУІБ) - це «та частина загальної системи управління організації, заснованої на оцінці бізнес ризиків, яка створює, реалізує, експлуатує, здійснює моніторинг, перегляд, супровід і вдосконалення інформаційної безпеки». Система управління включає в себе організаційну структуру, політики, планування, посадові обов'язки, практики, процедури, процеси і ресурси.

Створення та експлуатація СУІБ вимагає застосування такого ж підходу, як і будь-яка інша система управління. Використовувана в ISO 27001 для опису СУІБ процесна модель передбачає безперервний цикл заходів: планування, реалізацію, перевірку, дію (ПРПД).

Процес безперервного вдосконалення зазвичай вимагає початкового інвестування: документування діяльності, формалізація підходу до управління ризиками, визначення методів аналізу і виділення ресурсів. Ці заходи застосовуються для приведення циклу в дію. Вони не обов'язково повинні бути завершені, перш ніж будуть активовані стадії перегляду.

На стадії планування забезпечується правильне завдання контексту і масштабу СУІБ, оцінюються ризики інформаційної безпеки, пропонується відповідний план обробки цих ризиків. У свою чергу, на стадії реалізації впроваджуються прийняті рішення, які були визначені на стадії планування. На стадіях перевірки і дії посилюють, виправляють і вдосконалюють рішення з безпеки, які вже були визначені і реалізовані.

Перевірки можуть проводитися в будь-який час і з будь-якою періодичністю в залежності від конкретної ситуації. У деяких системах вони повинні бути вбудовані в автоматизовані процеси з метою забезпечення негайного виконання і реагування. Для інших процесів реагування потрібно тільки в разі інцидентів безпеки, коли в інформаційні ресурси, які підлягають захисту, були внесені зміни або доповнення, а також коли відбулися зміни загроз і уразливостей. Необхідні щорічні або іншої періодичності перевірки та/або аудити, щоб гарантувати, що система управління в цілому досягає своїх цілей.

Розглянемо методику побудови типової СУІБ на підприємстві чи в організації. Зауважимо, що нижченаведена методика не описує всіх особливостей експлуатації інформаційних систем в конкретній галузі функціонування, а є загальною і описує основні принципи побудови та впровадження СУІБ, що притаманні будь-якій системі.

Отже процес підготовки до побудови та сертифікації СУІБ умовно можна поділити на десять основних етапів:

- вибір процесів (сфери діяльності), які передбачається сертифікувати;
- формування робочого колективу (команди);
- проведення внутрішнього аудиту з метою визначення поточного стану інформаційної безпеки в підприємстві;
- проведення ідентифікації ресурсів, що входять до обраної сфери діяльності;
- визначення цінності ресурсів;

- визначення ризиків;
- розробка пакету документів (політики, стандарти, положення, процедури, інструкції тощо);
- проведення внутрішнього аудиту та оцінку створеної СУІБ з урахуванням здійсненої роботи із впровадження організаційних та технічних заходів;
- подання заявки на проведення сертифікаційного аудиту.

Нижче приведено короткий опис заходів, які здійснюються при виконанні кожного з десяти вищенаведених пунктів.

Вибір процесів (сфери діяльності), які передбачається сертифікувати, на перший погляд, є досить очевидним, однак фахівці в області інформаційної безпеки рекомендують тут користуватися принципом мінімальної достатності. До моменту затвердження галузі, що підлягає сертифікації рекомендується скласти перелік всіх існуючих бізнес-процесів на підприємстві та виокремити в ньому найбільш критичні з точки зору інформаційної безпеки. Як приклад це може бути обробка та зберігання персональних даних, інформація з обмеженим доступом, фінансові операції, інформація про розробки сфері інноваційних технологій тощо.

В якості найбільш ефективного способу визначення галузі бізнес-процесів, які будуть сертифіковані, використовується так званий чек-лист, який формалізовано представить всі процеси у відповідності до їх значимості.

На рис. 1 наведений приклад чек-листу бізнес-процесів підприємства.

№ з. п.	Назва бізнес-процесу	Короткий опис	Учасники бізнес-процесу	Задіяні інформаційні системи	Види інформації, що обробляється	Нормативно-правова база	Критичність (від 1 до 4)*	Важливість процесу (від 1 до 3)**

* 1 – висока;
2 – середня;
3 – низька;
4 – не впливає на процес.

**1 – важливий;
2 – маловажливий;
3 – не важливий.

Рис. 1. Приклад чек-листа, що описує бізнес-процеси підприємства

Побудова СУІБ – це комплексний процес, тому задіяти в ньому необхідно не тільки фахівців з інформаційної безпеки, а також співробітників підрозділів, що входять в сферу дії СУІБ. Як мінімум, в подальшому, ці співробітники повинні будуть відповідати на питання аудиторів на фінальному етапі проходження сертифікації. Нижче представлений типовий склад співробітників підприємства (можливо не тільки), що беруть участь у побудові СУІБ:

1. керівник підприємства;
2. адміністратор безпеки (відповідальний за безпеку інформації);
3. системний адміністратор;
4. директор з фінансів та розвитку;
5. секретар (відповідальний за роботу з документами, діловодство).

Мінімальна кількість членів робочої команди, як правило, становить три особи. Слід зазначити, що ці самі особи увійдуть до складу комісії з побудови СУІБ, що передбачає обговорення та прийняття рішень відносно здійснення тих чи інших заходів.

Проведення внутрішнього аудиту з метою визначення поточного стану інформаційної безпеки в підприємстві, серед інших заходів, передбачає аудит існуючих документів з інформаційної безпеки.

В табл. 1 наведений мінімальний перелік документів, необхідних для побудови СУІБ згідно з вимогами ISO/IEC 27001.

Таблиця 1

Перелік документів СУІБ згідно з вимогами ISO/IEC 27001

№ з.п.	Документи	Номер пункту стандарту
1.	Галузь дії	4.3
2.	Політика інформаційної безпеки	5.2, 6.2
3.	Методологія оцінки та обробки ризиків	6.1.2
4.	Положення про застосовуваність	6.1.3 d)
5.	План усунення ризиків	6.1.3 e), 6.2
6.	Звіт про оцінку ризиків	8.2
7.	Процедура управління документами	7.5
8.	Процедура управління записами	7.5
9.	Порядок внутрішнього аудиту	9.2
10.	Порядок та усунення несправностей	10.1
11.	Визначення ролей та обов'язків	A.7.1.2, A.13.2.4
12.	Матеріально-технічні ресурси активів	A.8.1.1
13.	Допустиме використання активів	A.8.1.3
14.	Політика управління доступом	A.9.1.1
15.	Процеси управління IT	A.12.1.1
16.	Принципи розробки захищеної системи	A.14.2.5
17.	Політика безпеки постачальника	A.15.1.1
18.	Процедура управління інцидентами	A.16.1.5
19.	Процедури неперервності бізнесу	A.17.1.2
20.	Юридичні, регулюючі та договірні вимоги	A.18.1.1
21.	Записи про ступінь підготовки, навички, досвід та кваліфікацію	7.2
22.	Моніторинг та вимірювання результатів	9.1
23.	Програма внутрішнього аудиту	9.2
24.	Результати внутрішніх аудитів	9.2
25.	Результати аналізів з боку керівництва	9.3
26.	Результати корегуючи дій	10.1
27.	Журнали дій користувачів, виключень та подій безпеки	A.12.4.1, A.12.4.3

Проведення ідентифікації ресурсів здійснюється з метою визначення та впорядкування інформації про всі ресурси, що задіяні в бізнес-процесах, які входять до галузі дії СУІБ. Інформація про наявні в організації ресурси узагальнюється в реєстрі ресурсів, який являє собою таблицю, форма якої наведена на рис. 2.

№ з.п.	Тип ресурсу	Власник ресурсу	Власник ризику	Користувач ресурсу	К	Ц	Д
	Інформація						
	Обладнання (комп'ютерне, прикладне, мережеве)						
	Програмне забезпечення						
	Сервіси (внутрішні зовнішні)						
	Персонал						
	Приміщення						

де:
К – конфіденційність;
Ц – цілісність;
Д – доступність.

Рис. 2. Форма реєстру ресурсів

Визначення цінності ресурсів полягає в оцінці критичності ресурсів підприємства з точки зору інформаційної безпеки за умовною шкалою, прийнятою на конкретному підприємстві (наприклад від 1 до 4, де «1» - це рівень цінності ресурсу, на якому його втрата або дискредитація ніяк не позначиться на інформаційній безпеці (найнижчий рівень цінності ресурсу), «4» – надвисокий рівень цінності ресурсу з точки зору інформаційної безпеки). Нижче приведена умовна шкала оцінки цінності ресурсів.

1 – втрата конфіденційності, цілісності та/або доступності ресурсу практично не призводить до фінансових, репутаційних, інформаційних чи інших втрат;

2 – втрата конфіденційності, цілісності та/або доступності ресурсу приводить до незначних втрат та здійснює незначний вплив на репутацію підприємства;

3 – втрата конфіденційності, цілісності та/або доступності ресурсу призводить до значних втрат та має значний вплив на репутацію підприємства;

4 – втрата конфіденційності, цілісності та/або доступності ресурсу призводить до великих втрат, має значний вплив на репутацію підприємства та може призвести до зупинки бізнес-процесу.

Методологія визначення ризиків полягає в їх оцінці та обробці. Існує декілька методів оцінки та обробки ризиків. Основним з них є, так званий, якісний метод.

Після визначення шкали цінності ресурсів необхідно визначити шкалу ступеню вразливості ресурсу. Наприклад ступінь вразливості від 1 до 4:

1 – вразливість практично не призводить до розкриття конфіденційної інформації;

2 – вразливість призводить до розкриття відомостей, які відносяться до інформації з обмеженим доступом, персональним даним тощо та призводить до втрат (фінансових, інформаційних, репутаційних тощо);

3 – вразливість призводить до розкриття відомостей, які відносяться до інформації з обмеженим доступом, персональним даним тощо та призводить до значних втрат, має значний вплив на репутацію підприємства та може призвести до зупинки бізнес-процесу;

4 – вразливість призводить до зупинки бізнес-процесу та порушення законодавства.

Також необхідно визначити частоту виникнення тієї чи іншої загрози, опираючись на власний досвід та досвід підприємства в цілому. Тут можливо також використовувати умовну шкалу від 1 до 4:

1 – загроза має місце в глобальному (історичному) контексті;

2 – загроза виникає 2-3 рази на рік в межах всієї галузі;

3 – загроза мала місце 1 раз на підприємстві;

4 – загроза проявляється 2-3 рази на рік на підприємстві.

Рівень ризику за окремими парами «загроза/вразливість» визначається множенням значень цінності ресурсу, його ступеню вразливості та частоти реалізації загрози:

$$Р=ЦР*СВ*Ч,$$

де:

ЦР – цінність ресурсу;

СВ – ступінь вразливості ресурсу;

Ч – частота реалізації загрози.

Загальний рівень ризику для ресурсу СУІБ підприємства дорівнює максимальному значенню із всіх ризиків по кожній парі «загроза/вразливість».

Стандарт ISO 27001 не містить в собі вичерпного переліку документів, тому розробка пакету документів у багатьох випадках є індивідуальною задачею для кожного окремого підприємства (організації). Багато документів, що потребуються при створенні СУІБ, є внутрішніми розпорядчими документами: накази, розпорядження, протоколи, акти тощо. Окрім документів, наведених в таблиці 1, мінімально необхідними є наступні організаційно-розпорядчі документи:

- наказ про створення та впровадження СУІБ;
- наказ про призначення відповідальних осіб;
- наказ про створення комісії з інформаційної безпеки.

Даний перелік не є вичерпним та може доповнюватись та змінюватись у відповідності до особливостей умов функціонування СУІБ на конкретному підприємстві.

Після здійснення всіх підготовчих заходів та розробки необхідних документів проводиться внутрішній аудит підприємства. При проведенні аудиту СУІБ важливо дотримуватись всіх принципів, що описані в стандарті ISO/IEC 27001. Внутрішній аудит може проводитись як співробітниками підприємства, так і сторонніми фахівцями. Однак слід пам'ятати, що в усіх питаннях, пов'язаних з аудитом СУІБ аудитор має бути незалежним від об'єкту аудиту. В цьому полягає фундаментальний сенс аудиту, як такого. Функція аудита на підприємстві повинна бути незалежною від галузі, що перевіряється, з метою отримання об'єктивних результатів.

Інформаційна безпека є областю, що динамічно розвивається, тому важливо, щоб аудитори інформаційної безпеки були обізнаними в галузі сучасних загроз, вразливостей та внутрішньої ситуації на підприємстві – бізнес-процесів, технологій, зв'язків.

Основними цілями внутрішнього аудиту є:

- визначення ступеню відповідності СУІБ підприємства та її складових частин стандарту ISO/IEC 27001;
- оцінка можливості СУІБ забезпечувати відповідність вимогам законодавчих та нормативно-правових актів, а також вимогам внутрішнього статуту та внутрішніх нормативно-розпорядчих документів підприємства;
- оцінка результативності СУІБ для досягнення конкретних цілей (наприклад тих, що визначені в політиці інформаційної безпеки, або в політиці СУІБ);
- ідентифікація напрямків потенційного розвитку вдосконалення СУІБ.

Результатом виконання всіх вищенаведених заходів є створення СУІБ на підприємстві та його підготовка до проведення зовнішнього аудиту з метою отримання відповідного сертифікату. Процес створення СУІБ закінчується поданням заявки на проведення зовнішнього аудиту до відповідного компетентного органу.

Аналізуючи вищенаведені заходи щодо підготовки та створення СУІБ на підприємстві можна дійти висновку, що наряду із створенням та впровадженням комплексних систем захисту інформації на об'єктах енергетичного сектору та об'єктах критичної інфраструктури, є доцільним також поступове створення та впровадження СУІБ на цих об'єктах. Це дозволить оптимізувати сили та ресурсний потенціал щодо досягнення оптимального рівня захищеності інформації з обмеженим доступом, гармонізувати галузь інформаційної безпеки на об'єктах критичної інфраструктури із світовими стандартами та, в перспективі, відмовитися від розбудови складних, дорогих та малоефективних комплексних систем захисту інформації.

Висновки

Доведено актуальність задачі розширення функціональних можливостей систем та комплексів інформаційної безпеки за рахунок впровадження СУІБ.

Проведено аналіз алгоритму створення СУІБ на об'єкті, де циркулює інформація з обмеженим доступом.

Наведено перелік, форма та зміст основних документів, що мають бути розроблені в процесі створення СУІБ.

Отримані результати дають можливість констатувати необхідність оптимізації систем захисту інформаційних ресурсів, які обробляються на об'єктах критичної інфраструктури, шляхом поступового впровадження на них СУІБ та поступового переходу від комплексних систем захисту інформації до систем управління інформаційною безпекою, як таких, що забезпечують більш ефективний та гнучкий захист інформації.

1. ISO27000 (ISO/IEC 27000:2009) «Інформаційні технології – Методи забезпечення безпеки – Системи управління інформаційною безпекою – Визначення та основні принципи»/
2. ISO27001 (ISO/IEC 27001:2013) «Інформаційні технології – Методи забезпечення безпеки – Системи менеджменту інформаційної безпеки – Вимоги».
3. ISO27002 (ISO/IEC 27002:2013) «Інформаційні технології – Методи забезпечення безпеки – Практичні правила управління інформаційною безпекою».
4. ISO27003 (ISO/IEC 27003:2010) «Інформаційні технології – Методи забезпечення безпеки – Керівництво з впровадження системи управління інформаційною безпекою».
5. ISO27004 (ISO/IEC 27004:2009) «Інформаційні технології – Методи забезпечення безпеки – Системи менеджменту інформаційної безпеки – Вимірювання».
6. ISO27005 (ISO/IEC 27005:2011) «Інформаційні технології – Методи забезпечення безпеки – Управління ризиками інформаційної безпеки».

Поступила 9.10.2017р.