УДК 681.3.06
DOI: 10.31673/2409-7292.2019.012127

В.М. Ахрамович, С.В. Амелькін

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ ПРИВАТНОГО ПІДПРИЄМСТВА. ОРГАНІЗАЦІЯ СЛУЖБИ ЗАХИСТУ ІНФОРМАЦІЇ ПРИВАТНОГО ПІДПРИЄМСТВА

Розглянуті основні компоненти підвищення ефективності системи захисту інформації приватного підприємства та організація служби захисту інформації приватного підприємства.

***Ключові слова*:** Служба захисту інформації.

Вступ

Перед сучасним приватним підприємством гостро стоять проблеми забезпечення інформаційної безпеки. Це пов'язано з розвитком інформатизації підприємства, з постійно зростаючою вартістю інформації, з одного боку, і активністю інформаційно-аналітичних структур і різного роду порушників, з іншого. Інформація обмеженого доступу використовується компаніями-конкурентами, шахраями, терористами у своїх корисливих цілях, завдаючи збитки підприємству – власникові цієї інформації.

Проблеми й завдання компаній сьогодні стали порівнянні із проблемами й завданнями цілих держав. Як і держави, вони співробітничають і воюють. Але війни тут називаються інформаційними: хто має інформацію, володіє якщо не світом, то фінансовими потоками. Як не дивно, але й сьогодні не всі керівники усвідомлюють нагальну потребу організації на їхньому підприємстві системи захисту комерційної таємниці. Серед тих, хто таку необхідність все-таки розуміє, чимало не знають, що слід робити, аби зберегти ті чи інші відомості в таємниці, з вигодою реалізувати їх, не зазнати збитків від їхнього витоку або втрати. Деякі йдуть тільки шляхом оснащення підприємства технічними засобами захисту, повністю ігноруючи організаційно-правові методи. Мається на увазі, зокрема, створення нормативно-правової бази, прийняття й суворе дотримання якої дозволять фірмі не лише зберегти й використати з вигодою свої секрети, але у разі витоку інформації мати підстави для подання позовної заяви.

Отже, тільки «комплексна система може гарантувати досягнення максимальної ефективності захисту інформації, тому що системність забезпечує необхідні складові захисту й установлює між ними логічний і технологічний зв'язок, а комплексність, що вимагає повноти цих складових, всеохоплення захисту, забезпечує її надійність» [1].

Система захисту інформації приватного підприємства

Метою системи захисту інформації підприємства є:

- запобігання витоку, розкраданню, втраті, перекручуванню, підробці інформації;
- запобігання загрозам безпеці особистості, підприємства, суспільства, держави;
- запобігання несанкціонованим діям щодо знищення, модифікації, перекручування, копіювання, блокування інформації;
- запобігання іншим формам незаконного втручання в інформаційні ресурси й системи, забезпечення правового режиму документованої інформації як об'єкта власності;
- захист конституційних прав громадян на збереження особистої таємниці й конфіденційності персональних даних, що існують в інформаційних системах;
- збереження конфіденційності документованої інформації відповідно до законодавства.

Для грамотної побудови й експлуатації системи захисту необхідно дотримуватись таких принципів її застосування :

- простота захисту;
- прийнятність захисту для користувачів;
- підконтрольність системи захисту;

- постійний контроль за найбільш важливою інформацією;
- дроблення конфіденційної інформації на складові елементи, доступ до яких мають різні користувачі;
- мінімізація привілеїв доступу до інформації;
- установка пасток для провокування несанкціонованих дій;
- незалежність системи керування для користувачів;
- стійкість захисту в часі й за несприятливих обставин;
- глибина захисту, його дублювання й перекриття;
- особлива персональна відповідальність осіб, що забезпечують безпеку інформації;
- мінімізація загальних механізмів захисту.

Алгоритм створення системи захисту конфіденційної інформації такий:

- визначення об'єктів захисту;
- виявлення загроз і оцінка їхньої ймовірності;
- оцінка можливої шкоди;
- огляд застосовуваних засобів захисту, визначення їхньої недостатності;
- визначення адекватних заходів захисту;
- організаційне, фінансове, юридичне та ін. види забезпечення засобів захисту;
- впровадження засобів захисту;
- контроль;
- моніторинг і коригування впроваджених засобів.

1. Начальник служби захисту інформації призначається наказом керівника підприємства. Він очолює групу компетентних співробітників, які висловлюють свої пропозиції щодо обсягу, рівня й способів забезпечення збереженості конфіденційної інформації.
2. Керівник групи, маючи відповідну кваліфікацію в цій сфері, із залученням окремих фахівців формує попередній список відомостей, які надалі ввійдуть в «Перелік відомостей, що становлять конфіденційну інформацію підприємства».
3 Керівник групи на основі цього списку визначає й подає на узгодження необхідні до захисту об'єкти (устаткування для обробки й обігу інформації, програмне забезпечення, комунікації для передання конфіденційних даних, носії інформації, персонал, допущений до роботи з використанням комерційної й іншої таємниці).
4 Аналізуються наявні засоби захисту відповідних об'єктів, визначається ступінь їхньої недостатності, неефективності, фізичного й морального зношування.
5 Вивчаються зафіксовані випадки спроб несанкціонованого доступу до захищених інформаційних ресурсів і розголошення інформації.
6 На основі досвіду підприємства, з використанням методу моделювання ситуацій група фахівців виявляє можливі шляхи несанкціонованих дій зі знищення інформації, її копіювання, модифікації, перекручування, використання й т. п. Загрози ранжуються за ступенем значимості й класифікуються за видами впливу.
7 На основі зібраних даних оцінюється можлива шкода підприємству від кожного виду загроз, що стає визначальним фактором для категорування відомостей в «Переліку» за ступенем важливості, наприклад, для службового користування, конфіденційно, суворо конфіденційно.
8 Визначаються сфери обігу кожного виду конфіденційної інформації: за носіями, територією поширення, допущеними користувачами. Для вирішення цього завдання група залучає керівників структурних підрозділів, вивчає їхні побажання.
9 Група проводить підготовку до введення зазначених засобів захисту.

Служба захисту інформації підприємства

Для забезпечення працездатності розробленої системи захисту інформації необхідно створити спеціальний відділ у складі організації, що займається даними питаннями, – Службу захисту інформації (СЗІ).

До завдань СлЗІ належить:

- своєчасне виявлення загроз інформації, яка захищається, причин і умов їхнього виникнення й реалізації;
- виявлення й максимальне перекриття потенційно можливих каналів і методів несанкціонованого доступу до інформації;
- відпрацьовування механізмів оперативного реагування на загрози, використання юридичних, економічних, організаційних, соціально-психологічних, інженерно-технічних засобів і методів виявлення й нейтралізації джерел загроз безпеці компанії;
- організація спеціального діловодства, що виключає несанкціоноване одержання конфіденційної інформації.

Начальник СЗІ є новою штатною одиницею. На цю посаду слід брати професіонала-фахівця в галузі захисту інформації, котрий добре знає юридичний бік цієї проблеми, має досвід керівництва й координації роботи аналогічних служб. Вимоги: вища професійна освіта й стаж роботи в галузі захисту інформації не менше 5 років, знання законодавства в цій сфері, принципів планування захисту.

Начальник СЗІ повинен виконувати такі функції:

- виробляти політику забезпечення захисту інформації й забезпечувати її реалізацію;
- відповідати за функціонування СлЗІ й забезпечення захисту конфіденційної інформації;
- здійснювати планування й безпосереднє керівництво роботою СлЗІ, нести персональну відповідальність за виконання службою покладених на неї завдань, за неухильне виконання підлеглими своїх посадових обов'язків і правил внутрішнього трудового розпорядку;
- брати особисту участь у проведенні найбільш складних заходів щодо забезпечення захисту інформації в компанії;
- розробляти плани дій у надзвичайних ситуаціях, регулярно проводити навчання з підлеглими;
- керувати проведенням службових розслідувань;
- організовувати взаємодію СлЗІ з іншими підрозділами;
- розробляти інструкції з роботи з комерційною таємницею для персоналу, допущеного до роботи з відповідними документами;
- організовувати розробку рекомендацій з удосконалювання функціонування СлЗІ;
- здійснювати керівництво відділом охорони;
- крім того, виконувати функції юриста: розробка, ведення й оновлення основних документів з метою закріплення в них вимог забезпечення безпеки й захисту конфіденційної інформації.

Підрозділ програмно-апаратного захисту інформації.

Цілями захисту інформації, яка обробляється й зберігається в ПЕОМ, є:

1. запобігання втраті й витоку інформації, перехопленню й втручанню зловмисника на всіх рівнях обробки даних і для всіх об'єктів;
2. забезпечення цілісності даних на всіх етапах їхнього перетворення й збереження засобів програмного забезпечення.

Завдання підрозділу:

- запобігання несанкціонованому доступу (НСД) до інформації;
- запобігання витоку інформації за рахунок побічних електромагнітних випромінювань (ПЕМВ);

- захист інформації від комп'ютерних вірусів;
- захист інформації від збоїв у системі живлення;
- захист від копіювання;
- програмний захист каналів передачі даних.

Підрозділ інженерно-технічного захисту інформації.

Інженерно-технічний захист інформації призначений для активно-пасивних протидій засобам технічної розвідки й формування рубежів охорони території, будинків, приміщень, устаткування за допомогою комплексів технічних засобів і містить:

- споруди фізичного (інженерного) захисту від проникнення сторонніх осіб на територію, у будинки й приміщення;
- засоби захисту технічних каналів витоку інформації при роботі ЕОМ, засобів зв'язку, інших приладів і офісного устаткування при проведенні нарад, бесід з відвідувачами й співробітниками;
- засоби захисту приміщень від візуальних засобів технічної розвідки;
- засоби забезпечення охорони територій, будинків, приміщень;
- засоби протипожежної охорони;
- технічні засоби й заходи, що запобігають винесенню персоналом із приміщень документів, дискет, дисків та інших носіїв інформації.

Підрозділ конфіденційного діловодства.

Завдання:

- обробка й зберігання конфіденційних документів;
- контроль системи конфіденційного документообігу.

У не дуже великих організаціях доцільно організувати СЗІ в такому складі:

- начальник СЗІ;
- співробітник, що займається програмно-апаратним захистом;
- співробітник, що займається інженерно-технічним захистом.

Функції конфіденційного діловодства покласти на вже наявних співробітників, котрим на цей час доручено створення й обробка документів, що містять конфіденційну інформацію.

Пакет документів для роботи СЗІ

Для роботи СЗІ необхідно підготувати ряд нормативних документів:

- положення про СлЗІ;
- інструкцію з безпеки конфіденційної інформації;
- перелік відомостей, що становлять конфіденційну інформацію;
- інструкцію з роботи з конфіденційною інформацією;
- посадові інструкції співробітників СлЗІ;
- інструкцію із забезпечення пропускного режиму в компанії;
- пам'ятку працівникові (службовцеві) про збереження конфіденційної інформації**.**

Для забезпечення повноцінного організаційного й правового захисту інформації необхідно розробити пакет документів, а саме:

- положення про конфіденційну інформацію підприємства;
- перелік документів підприємства, що містять конфіденційну інформацію;
- інструкцію із захисту конфіденційної інформації в інформаційній системі підприємства;
- пропозиції щодо внесення змін до Статуту підприємства;
- пропозиції щодо внесення змін до трудового договору, контракту із керівником і колективного договору;
- угоду зі співробітником про нерозголошення конфіденційної інформації підприємства;
- зобов'язання співробітника про нерозголошення конфіденційної інформації підприємства після звільнення;

- пропозиції щодо внесення змін до Правил внутрішнього розпорядку підприємства (у частині регламентації засобів фізичного захисту інформації й питань режиму);
- пропозиції щодо внесення змін до посадового (штатного) розкладу підприємства (штату Служби захисту інформації);
- пропозиції щодо внесення доповнень до посадових інструкцій усього персоналу;
- відомість ознайомлення співробітників підприємства з Положенням про конфіденційну інформацію й Інструкцію із захисту конфіденційної інформації в інформаційній системі підприємства;
- план проведення занять із персоналом щодо збереження й нерозголошення конфіденційної інформації;
- пропозиції щодо внесення змін до структури інтерв'ю при прийманні на роботу (уточнення зобов'язань інформаційного характеру з останніх місць роботи);
- пропозиції щодо внесення доповнень до стандартних договорів з контрагентами.

Ці документи відіграють важливу роль у забезпеченні безпеки підприємства.

Документаційнє забезпечення захисту починається з внесення доповнень до Статуту підприємства: «Підприємство має право самостійно встановлювати обсяг відомостей, що становлять комерційну й іншу охоронювану законом таємницю й порядок її захисту. Підприємство має право з метою захисту економічного суверенітету вимагати від персоналу, партнерів, контрагентів та інших фізичних і юридичних осіб, установ і організацій забезпечення нерозголошення конфіденційних відомостей підприємства на підставі договорів, контрактів та інших документів».

Для розробки всіх документів, які стосуються роботи з конфіденційною інформацією, необхідно в першу чергу розробити «Положення про конфіденційну інформацію». Формат усіх документів, що регулюють захист конфіденційної інформації, затверджується наказом керівника. Положення ж є основним документом підприємства, котрий регламентує питання обігу конфіденційної інформації. Всі базові моменти, пов'язані із цим процесом, застерігаються саме тут.

Положення містить основні обов'язки співробітників з забезпечення збереженості конфіденційної інформації. Для посилення цієї складової системи захисту необхідно обов'язки доводити персоналу також у формі включення в посадові інструкції, додатково видавати спеціальні пам'ятки. Все це має відбуватися виключно під розпис.

Невід'ємним додатком до Положення є Перелік документів, що містять конфіденційну інформацію. Його наявність на підприємстві має принциповий характер, тому що неможливо вимагати від працівників нерозголошення абстрактної конфіденційної інформації, як іноді вказують у зобов'язальних документах: «зберігати ноу-хау, ділові секрети, службові відомості». Захищається тільки документована інформація, а тому, необхідно якомога конкретніше описати всі групи й види конфіденційної документації.

За основу для встановлення контролю над доступом до інформації компанії береться класифікація інформації за рівнем конфіденційності, залежно від змісту й можливих наслідків у разі втрати інформації або зловживань.

За категоріями конфіденційності основні види інформації розподіляються приблизно так:

Найнижчий гриф конфіденційності «ДСК» ставиться на телефонні довідники, де є окремі дані про кадровий склад або партнерів. Цей гриф також ставиться на журнали реєстрації, документи, що регламентують діяльність, службове листування (заяви, розпорядження, накази, доповідні й т. д.).

До категорії документів із грифом "КОНФІДЕНЦІЙНО" належать ті, де міститься інформація про окремі аспекти ділових угод за короткий проміжок часу; розгорнуті відомості про персонал компанії; про поточну фінансову діяльність; дані про клієнтуру, які не надаються третім особам.

Гриф "СУВОРО КОНФІДЕНЦІЙНО" присвоюється документам, що містять дані про ділові угоди з партнерами або клієнтами фірми, про підсумки діяльності за тривалий період часу. Крім цього, цей гриф надається документам про найважливіші аспекти комерційної діяльності компанії, стратегію діяльності, документам, що містять детальну інформацію про фінансове становище.

Класифікації за рівнем конфіденційності підлягають усі документи відповідно до плану заходів щодо забезпечення безпеки компанії. Питання про присвоєння грифа вирішується розробником документа за участю начальника СлЗІ. Якщо цінність інформації з яких-небудь причин знижується, знижується й гриф документа.

Окремої уваги заслуговує питання про терміни дії грифів конфіденційності. Строк таємності визначається автором документа, виконавцем, особою, що підписує або затверджує документ за узгодженням керівником СлЗІ. Строк може вказуватися у вигляді періоду грифа, з дати закінчення грифа, настання певної події, на яку зорієнтований документ, або напису «безстроково». У деяких випадках рішення, щодо зняття грифа залишається за начальником СлЗІ.

Наступний документ, що входить до складу документації впровадження, – **угода зі співробітником (зобов'язання співробітника) про нерозголошення конфіденційної інформації підприємства**, яку співробітник підписує при зарахуванні на роботу. Угода містить:

- зобов'язання про збереження конфіденційної інформації;
- право співробітника на службовий добуток;
- відповідальність співробітника за порушення даного зобов'язання.

Перед підписанням зобов'язання доцільно також ознайомлювати кандидатів із витягами з законодавства, які коротко обґрунтовують правовий захист і санкції за неправомірне поводження з інформацією, у тому числі -кримінально-правові.

Продовженням обов'язків співробітника з нерозголошення інформації є «Заява про підтвердження зобов'язань нерозголошення конфіденційної інформації підприємства при звільненні».

Документ не є бездоганним з юридичної точки зору, тому що після звільнення трудові відносини, в межах яких діють зобов'язання співробітника, припиняються. Однак доцільно пропонувати співробітнику, що звільняється, підписати таку заяву: за його реакцією можна буде оцінити реальну значимість для конкретної людини даних їм обіцянок. У той же час, у разі завдання збитків підприємству від розголошення звільненим конфіденційних відомостей таке зобов'язання, швидше за все, буде прийняте судом як додатковий доказ його провини. Крім того, про це можна буде з чистим сумлінням повідомити його новому роботодавцеві.

Ставлення контрагентів і партнерів до таємниці організації слід виявляти самій організації. Для цього необхідно внести в усі стандартні форми договірної документації розділи щодо конфіденційності:

9. Кожна зі сторін погодилася вважати текст даного договору, а також весь обсяг інформації, що передається сторонами одна одній під час виконання зобов'язань, що виникають із даного договору, конфіденційною інформацією іншої сторони.

10. Сторони зобов'язуються не розголошувати в будь-який спосіб (робити доступною третім особам, крім випадків наявності в третіх осіб відповідних повноважень у силу прямої дії закону, або випадків, коли інша сторона в письмовій формі дасть згоду на надання конфіденційної інформації, обумовленою відповідно до п. 1 даного договору, третім особам) конфіденційну інформацію іншої сторони, до якої вона одержала доступ при укладанні даного договору й у ході виконання зобов'язань, що виникають із нього.

11. Ці зобов'язання виконуються сторонами в межах терміну дії договору й протягом одного року після припинення дії договору, якщо не буде обумовлене інше.

12. Кожна зі сторін зобов'язується відшкодувати іншій стороні в повному обсязі всі збитки, заподіяні останній розголошенням її конфіденційної інформації в порушення п. п. 1 – 3 цього договору.
13. Клієнт (постачальник та ін.) не вправі використати своє становище як сторони за даним договором в цілях і інтересах третіх осіб.
14. Сторони зобов'язуються негайно попередити іншу сторону про виникнення некерованих факторів або процесів, що можуть спричинити порушення конфіденційності сторін.
Служба захисту інформації вживає заходів щодо збереження комерційної таємниці шляхом максимального обмеження кола осіб, які мають до неї доступ, фізичної збереженості документів, що містять такі відомості, обробки інформації із грифом конфіденційності на захищених ЕОМ, внесення вимог щодо конфіденційності конкретної інформації в договори із внутрішніми й зовнішніми партнерами та інших заходів за рішенням керівництва.
Усі роботи з документами, що містять конфіденційну інформацію, регламентуються положенням про конфіденційне діловодство.
Захист і обробка конфіденційних документів передбачають:

- порядок визначення інформації, що містить комерційну таємницю, і строків дії відповідних грифів;
- систему допуску співробітників, відряджених і фізичних осіб до відомостей, що становлять комерційну таємницю;
- забезпечення збереження документів на паперових і магнітних носіях з грифом конфіденційності;
- обов'язки осіб, допущених до відомостей, що становлять комерційну таємницю;
- принципи організації й проведення контролю за забезпеченням режиму при роботі з відомостями, що становить комерційну таємницю;
- відповідальність за розголошення відомостей, втрату документів, що містять комерційну таємницю.

Допуск співробітників до відомостей, що становлять комерційну таємницю, здійснюється Генеральним директором і начальником СЗІ.
Начальник СЗІ, відповідальний за підбор осіб, що допускаються до відомостей з грифом, зобов'язаний забезпечити контроль за тим, щоб до цих відомостей одержували доступ тільки ті особи, яким такі відомості необхідні для виконання своїх службових обов'язків.

Висновок

В сучасному інформаційному просторі вже неможливо успішне функціонування об’єктів інформаційної діяльності без управління процесами інформаційної безпеки.
Капіталовкладення в захист інформації є важливим інвестиціями в майбутній розвиток інформаційної безпеки.
Зважаючи на розвиток будь-якого підприємства, відділ захисту інформації, це повноцінний підрозділ організації яке відповідає за кібербезпеку компанії.
Враховуючи всі негативні процеси в теперішній час захист інформації є невід’ємною ланкою майже всіх суб’єктів господарювання
Кожний співробітник незалежно від свого службового становища або ступеня спорідненості з керівником підприємства повинен володіти тільки тією інформацією, якому йому необхідна для роботи.

Список літератури:

1. Ахрамович. В.М. Ідентифікація й аутентифікація, керування доступом. Сучасний захист інформації. К. ДУТ:-2016 .-№4.- с. 47-51
2. Ахрамович. В.М. Адміністративний рівень інформаційної безпеки. Сучасний захист інформації. К. ДУТ:-2017 .-№1.- с. 10-14
3. В.М. Ахрамович, В.М. Чегренець. Інформаційна безпека. Практикум/ В.М. Ахрамович, В.М. Чегренець.-К.: ДУТ, 2017.-396с