фишинг, вирусы и т.д.; Agava Spamprotexx - интеллектуальный спам-фильтр которой работает быстро, эффективно и максимально лёгок в использовании.

Выводы

Во времена разработки базовых почтовых протоколов первоочередной задачей была передача почтовых сообщений, а не защита от злоумышленников, конечно протоколы постепенно дорабатываются, появляются новые механизмы аутентификации, однако в силу децентрализованной природы интернета их внедрение требует времени.

Почта каждого человека очень индивидуальна и зависит от области интересов, деятельности и т.д. Что считать спамом или не-спамом — решает только конкретный пользователь. Системный администратор, в свою очередь, должен вести тщательно продуманную политику обработки почты, включающую не только уничтожение спама, но маршрутизацию и хранение незапрошенной и даже нежелательной почты.

УДК 004.681

Сєрєнко В.Є.

ВИЗНАЧЕННЯ ІНФОРМАЦІЇ, ЩО ПІДЛЯГАЄ ЗАХИСТУ – ПЕРШИЙ ЕТАП ПРИ ПОБУДОВІ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

Вступ

Захист інформації на підприємстві починається з визначення самої інформації, втрата, порушення цілісності або доступності якої можуть призвести до непередбачених фінансових витрат та завдати маральної чи фізичної шкоди.

Організацією процесу визначення інформації на підприємстві повинен займатися підрозділ, на якого покладено функції з адміністрування процесами управління підприємством, та який має організаційно-розпорядчий вплив на всі структурні підрозділи підприємства (як приклад служба забезпечення діяльності керівника підприємства).

Вихідними даними даного етапу є аналітична інформація про інформаційну систему підприємства, що використовується підрозділом захисту інформації підприємства у подальшому, при створенні комплексної системи захисту інформації.

Класифікатор інформації

Основним організаційним документом, який регулює діяльність підприємства у сфері інформаційних відносин є класифікатор інформації.

Класифікатор інформації – це офіційний документ, який в загальних рисах описує інформаційну систему підприємства.

Формують класифікатор інформації структурні підрозділи підприємства, спираючись на положення про підрозділи (функціональні обов'язки підрозділу).

Формування класифікатору проходить в три етапи (як приклад рис. 1):

- на першому етапі структурні підрозділи підприємства подають відомості до класифікатору стосовно інформації, яку вони використовують при виконанні своїх функціональних обов'язків. При цьому вказані структурні підрозділи визначаються як *користувачі* поданої інформації;
- на другому етапі структурні підрозділи подають відомості до класифікатору стосовно інформації, яку вони отримують на виході при виконанні своїх функціональних обов'язків. При цьому вказані структурні підрозділи визначаються як *джерела* поданої інформації;
-

Таблиця 1 – Класифікатор інформації на підприємстві

Об'єкт інформаційних відносин			Суб'єкт інформаційний відносин				
№ з/п	Вид інформації	Опис інформації	Суб'єкт права власності на інформацію (нормативне закріплення правомочностей)				Джерело інформації
			Власник	Володілець	Користувач	Розпорядник	
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1	Правова інформація	Відомості, стосовно порядку створення КСЗІ в органах державної влади	Держава (ст. 38 ЗУ «Про інформацію»)	ДПА України	Підрозділ захисту інформації ДПА України, інші структурні підрозділи, при необхідності	Держава	ВРУ, Президент України, КМУ, СБУ, Держспецзв'язок
2	Правова інформація	Відомості, стосовно порядку створення КСЗІ в органах ДПС України	Держава (ст. 38 ЗУ «Про інформацію»)	ДПА України	Структурні підрозділи ДПА України, підрозділи органів ДПС України, при необхідності	Держава	Підрозділ захисту інформації ДПА України

- при формуванні класифікатору додатково залучається підрозділ захисту інформації (як правило РСО) підприємства, який коригує класифікатор відповідно до ЗВДТ, що сприяє формуванню повноти класифікатору.
- До правової бази для створення класифікатору інформації на підприємстві можна віднести:
- Цивільний Кодекс України;
- Закон України "Про інформацію";
- Статут підприємства;
- Положення про структурні підрозділи підприємства.

На основі класифікатору інформації готуються:

- перелік конфіденційної інформації, що є власністю держави на підприємстві (Постанова КМУ від 27 листопада 1998 р. № 1893 "Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави");
- перелік конфіденційної інформації, що є власністю фізичних або юридичних осіб;
- перелік інформації, яка підлягає захисту (на кожному об'єкті інформаційної діяльності, в кожній автоматизованій системі).

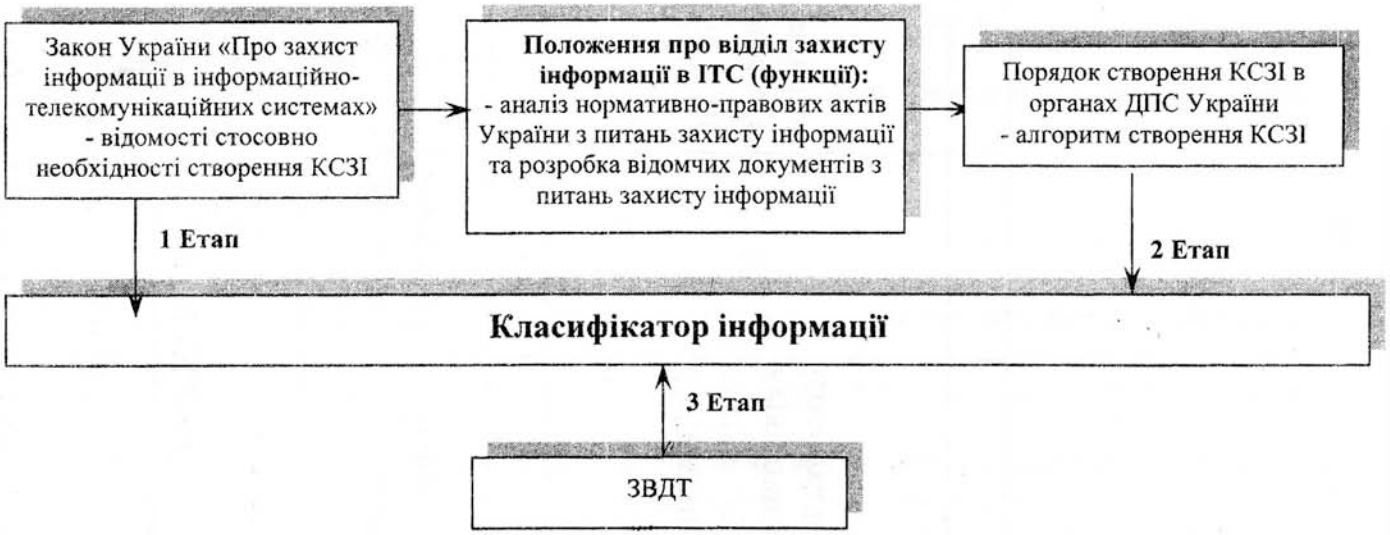

Рис 1. формування класифікатору інформації відділом захисту інформації в ІТС

Об'єкт інформаційних відносин – інформація, як відомості про осіб, предмети, факти, події, явища та процеси незалежно від форми їх представлення в інформаційній системі.

Вид інформації (відповідно до статті 18 Закону України «Про інформацію»):

- статистична інформація;
- адміністративна інформація (дані);
- масова інформація;
- інформація про діяльність державних органів влади та органів
- місцевого і регіонального самоврядування;
- правова інформація;
- інформація про особу;
- інформація довідково-енциклопедичного характеру;
- соціологічна інформація.

Опис інформації – формальний опис відомостей, з якими працює підрозділ підприємства.

Перелік інформації, що підлягає захисту в інформаційній системі

Повна назва ОІД/АС (_____) Власник ОІД/АС: _____
(скорочена назва ОІД/АС)

№ з/п	Відповідний номер класифікатора інформації	Детальний опис інформації	Категорія інформації	Вид оброблення інформації в системі	Носій (-ії) інформації
1	*2*	*3*	*4*	*5*	*6*
1	2	Порядок створення КСЗІ в АС 1 класу органів ДПС України, призначених для обробки секретної інформації	4	Збереження інформації на носіях у робочий та неробочий час; Обробка в АС	Автоматизована система (жорсткий диск № 10 ДСК); Дискета (Обл. № 13ДСК); Папір; Люди, які працюють або працювали з даною інформацією

Деталізація опису інформації на даному етапі не важлива, оскільки це буде зроблено з визначенням носіїв інформації на етапі створення переліку інформації, яка підлягає захисту.

Суб'єкт інформаційних відносин – особа, фізична чи юридична, якій належать ті чи інші права та обов'язки, що виникають при взаємодії з іншими особами в інформаційній системі.

Суб'єкт права власності на інформацію

Суб'єктивне право власності формується як сукупність трьох найголовніших правомочностей: права володіння, права користування, права розпорядження.

Довідка:

право володіння інформацією – це закріплена у нормах права можливість фактичного володіння інформацією: фізичного або господарського, оскільки однаково володіє інформацією той, хто утримує її фізично (наприклад, орган державної влади, який накопичує інформацію про громадян в своїх банках даних), а також той, хто має змогу впливати на цю інформацію (наприклад, громадянин, який надає в установленій формі інформацію про себе органам державної влади не може володіти нею у фізичному розумінні, але він здійснює правомочність володіння внаслідок того, що має змогу впливати на цю інформацію);

право користування – це закріплена нормами права можливість вилучення корисних властивостей інформації для задоволення потреб власника чи інших осіб;

право розпорядження інформацією – це закріплена у нормах права можливість визначити юридичну чи фактичну долю інформації

В залежності від того, які права по відношенню до інформації застосовують суб'єкти права власності можна виділити:

власників інформації

- володільців;
- користувачів інформації;
- розпорядників.

Правомочності з користування, володіння і розпорядження виникають у власника водночас з виникненням права власності, а сукупність (тріада) цих правомочностей, яка характеризує право власності у повному обсязі і розкриває його зміст, може належати лише власнику і нікому більше.

Разом з тим право володіння власника відрізняється від права володіння інших осіб – титульних володільців, оскільки власник здійснює цю правомочність, як правило, у сукупності з іншими – правом користування і розпорядження. Крім того, власник робить це незалежно від інших осіб. Щодо титульних володільців, то вони мають узгоджувати свої дії з власником або здійснювати володіння на підставі договору, адміністративного акта, закону.

Право користування нерозривно пов'язано з правом володіння. Без володіння, тобто без фактичного утримання інформації, не можна добути з неї корисні властивості і тим самим використати її для задоволення потреб. Користувачем інформації може бути не лише її власник, а й інші суб'єкти, яким це право належить на правових підставах (описано порядок

вилучення корисних властивостей інформації для задоволення потреб власника чи інших суб'єктів). Як приклад, структурний підрозділ (користувач) органу державної влади (володілець),

користуючись інформацією баз даних (інформація про громадян) свого підприємства, проводить аналітичну роботу та готує прогнозні показники (виконує функціональні обов'язки).

Якщо вищевикладені правомочності володіння і користування можуть належати не лише власникові, а й іншим суб'єктам, то право розпоряджатися інформацією належить, як правило, лише власнику цієї інформації. Винятки становлять випадки примусового вилучення інформації у власника або володільця.

Джерелом інформації, якою володіє, користується та/або розпоряджається підприємство можуть бути:

- інститути гілок влади:
  - законодавчою: Верховна Рада України, Президент України, тощо;
  - виконавчої: Кабінет міністрів України, міністерства, центральні органи виконавчої влади, тощо;
  - судової: Конституційний Суд України, Верховний Суд України, Вищий адміністративний суд України, Вищий господарський суд України, тощо;
  - інші організації, установи та підприємства державної форми власності
- юридичні особи не державної форми власності;
- фізичні особи;
- громадяни України;
- особи без громадянства;
- міжнародні організації;
- іноземні представництва;
- тощо.

У разі здійснення підприємством систематичних інформаційних відносин з певним джерелом інформації та при відсутності встановлених правил обміну інформацією між ними, необхідно ці правила розробити та впровадити в установленому порядку. Правила обміну інформацією повинні обов'язково визначати:

- формальний опис інформації (вид, режим доступу);
- носії інформації та форма її представлення;
- технологію передачі інформації
- джерело та отримувача інформації:
- найменування, форма власності;
- права власності джерела та отримувача на інформацію (власник, розпорядник або користувач інформації)
- тощо.

Обмін інформацією може бути як одностороннім так і двостороннім.

При здійсненні одностороннього обміну відповідальним за розробку Правил обміну інформацією між джерелом та отримувачем (та розробку комплексної системи захисту в ІТС, у разі якщо обмін здійснюється автоматизованим шляхом) повинен бути отримувач інформації, якщо інше не передбачено угодою з обміну.

У разі вчинення двостороннього обміну інформацією між двома суб'єктами інформаційних відносин, які одночасно є і джерелом інформації і її отримувачем, відповідальність за розробку Правил обміну інформацією (та розробку комплексної системи захисту в ІТС, у разі якщо обмін здійснюється автоматизованим шляхом) закріплюється угодою з обміну та визначається:

- спільним рішенням суб'єктів інформаційних відносин (перевага з призначення відповідальним лежить на боці суб'єкта, який перший ініціював обмін);
- рішення третьої сторони, що є обов'язковим для виконання вказаними суб'єктами інформаційних відносин.

Категорія інформації – це відносний показник, що вказує на важливість інформації. Він вводиться для того, щоб вказати підрозділу захисту інформації на властивості інформації, які необхідно захищати.

Значення від 1 до 3 вказують на те, що інформація має гриф секретності "Особливо важлива", "Цілком таємно" та "Таємна" відповідно. Значення 4 – інформацію віднесено до обмеженого доступу та надано статус конфіденційної інформації або присвоєно гриф обмеження доступу "Для службового користування". Для категорій інформації від 1 до 4 обов'язково необхідно захищати конфіденційність, цілісність та доступність інформації при цьому додатково можуть висуватися вимоги до спостережності інформації. Значення 5 казує

на те, що інформація є відкритою та потребує захисту від порушення цілісності та доступності. Значення 6 – інформація є відкритою та не потребує захисту.

Видами оброблення інформації в системі можуть бути:

- обговорення;
- оброблення в АС;
- оброблення технічними засобами (крім тих, що входять до складу АС);
- збереження на різних носіях в пасивному стані (постійно чи тимчасово).

Носії інформації:

- акустичні поля;
- електромагнітні поля радіодіапазону;
- електричні сигнали в струмопровідних комунікаціях;
- електромагнітні поля в інфрачервоній, видимій та ультрафіолетовій частині спектра;
- матеріально-речові носії: папір, фото, магнітні та оптичні носії, використаний матеріал, тощо;
- до того ж одним з носіїв інформації є людина.

На сьогоднішній день людина є одним з найпоширеніших носіїв інформації, який тяжко контролювати на предмет витоку інформації. Тому службі захисту інформації слід уділяти особливу увагу при роботі з фахівцями підприємства:

- проводити бесіди з робітниками підприємства з питань відповідальності за розголошення інформації з обмеженим доступом;
- готувати навчальні посібники, методичні матеріали з правил обробки інформації, використання носіїв інформації, тощо;
- брати розписки з робітників підприємства про нерозголошення отриманої для роботи інформації і т. ін.

Висновки

Сучасна політики безпеки інформації, описана нормативно-правовими актами України в галузі захисту інформації, направлена на захист саме носіїв інформації а не конкретної інформації. Свідчення тому наступні:

- відсутній в законодавчих актах України алгоритм формування переліку та класифікатору інформації в органах державної влади, на підприємствах, в установах різних форм власності та діяльності;
- перевірка виконання вимог із захисту інформації на підприємстві контролюючим органом проводиться на конкретному об'єкті інформаційної діяльності в конкретній автоматизованій системі. Роботи з виявлення джерел, користувачів конкретної інформації не ведуться. Наявність аналогічної інформації на інших носіях підприємства також не перевіряється.

Вказаний підхід дозволить з певною долею вірогідності захистити носій інформації, а відповідно і інформацію, яка на ньому знаходиться від:

- його викрадання;
- неконтрольованого доступу до нього;
- руйнування, знищення;
- і т. ін.

Але не дозволить запобігти витоку цієї ж інформації з іншого, незахищеного носія, т. я. носій цей не було прийнято до уваги службою захисту.

Саме впровадження та підтримання на підприємстві класифікатора інформації, переліку інформації, що потребує захисту дозволить вирішити порушені проблемні питання, та приступити до виконання наступного етапу створення комплексної системи захисту інформації - "Виявлення загроз та каналів витоку інформації".

Надійшла 19.12.2007р.