Захист інформації та кібернетична безпека

УДК 004.056 DOI: 10.30748/soi.2018.153.15

Ю.В. Борсуковський[1], В.Ю. Борсуковська[2], В.Л. Бурячок[3], П.М. Складанний[3]

[1] *Державний університет телекомунікацій, Київ*
[2] *ПАТ «Укрсоцбанк», Київ*
[3] *Київський університет ім. Бориса Грінченка, Київ*

ПРИКЛАДНІ АСПЕКТИ РОЗРОБКИ ПОЛІТИКИ КАТЕГОРУВАННЯ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

В статті проведено детальний аналіз прикладних аспектів розробки політики інформаційної безпеки щодо категорування інформації з обмеженим доступом для корпоративних користувачів, які починають впроваджувати автоматизовані DLP та DAG системи. З урахуванням того, що у вітчизняному законодавстві чітке розуміння поняття «комерційна таємниця» відсутнє, а кожен власник підприємства може самостійно визначати перелік інформації, яка для нього та підприємства в цілому є конфіденційною, а також самостійно визначати порядок роботи з такою інформацією, в статті, по-перше, сформульовано базові вимоги та рекомендації щодо структури та змісту типової політики категорування інформації з обмеженим доступом для підприємств різних форм власності й, по-друге, введено низку нових понять, які дозволять уникнути конфлікту при впровадженні DLP та DAG систем з певними їх трактуваннями, визначеними на законодавчому рівні. Як результат, це сприятиме суттєвому зменшенню ризиків, пов'язаних з несанкціонованим доступом до конфіденційної інформації, знищенням інформаційних ресурсів, компрометації інформаційних ресурсів підприємства. Разом з тим, у статті розглянуто приклад категорування інформації з обмеженим доступом; визначено вимоги щодо формування реєстру інформаційних активів та сформовано практичні рекомендації щодо категорування інформації із врахуванням досвіду впровадження систем управління доступом до неструктурованих даних та систем запобігання витокам інформації.

Ключові слова: *категорування, класифікація, доступ, політика, кібербезпека.*

Вступ і постановка задачі

Категорування інформації в корпоративних інформаційних ресурсах (ІР) є ключовою функцією забезпечення інформаційної безпеки (ІБ) [3–5]. Дане завдання в тому чи іншому вигляді вирішується в кожній інформаційній системі (ІС) підприємств державного та приватного сектору і формалізуєтеся у відповідній політиці ІБ підприємства. Завдяки процесу зіставлення категорій інформації і прав користувачів забезпечується процес захисту інформації з обмеженим доступом (ІзОД) від несанкціонованого використання [1–2].

У корпоративній мережі кожного підприємства зберігається і обробляється інформація, яка є критичною для ведення бізнесу і може власником відноситься до комерційної та/або службової таємниці підприємства, інформація щодо персональних даних співробітників, а також інша конфіденційна інформація підприємства, доступ до якої може обмежуватися її власником. Виходячи з досвіду впровадження DLP та DAG систем, на суб'єктивну думку авторів, діюче законодавство не відповідає сучасним викликам та загрозам інформаційним активам підприємств. Наочною демонстрацією може служити атака на українські інформаційні ресурси шифрувальника notPetya. Аналіз передумов та наслідків однозначно показує необхідність проведення кардинальних змін та доповнень у чинному законодавстві у відповідності до існуючого та прогнозованого ландшафту інформаційних та кібернетичних загроз. Очевидно, що частина проблемних питань може бути вирішена простою імплементацією діючих міжнародних стандартів, а не придумуванням своїх, що, як показують останні сумні наслідки, не завжди є кращими, а в багатьох випадках обмежують використання сучасних засобів протидії зловмисникам. Очевидно, що у відповідності до доктрин відносно питань інформаційної та кібернетичної безпеки, що прийняті провідними країнами світу ми повинні розглядати загрози інформаційним ресурсам підприємствам не тільки в кримінальному аспекті, а і в глобальному – як боротьба за вплив в інформаційному просторі.

Одне із питань, що потребує достатньо прискіпливого підходу при розробці політик інформаційної безпеки при впровадженні DLP та DAG систем – це категорування інформації, що власником відноситься до ІзОД підприємства. З цією метою для забезпечення захисту ІР від їх незаконного використання повинна бути розроблена на підприємстві політика інформаційної безпеки (ПІБ) [6–7] щодо порядку доступу до ІзОД, а також формалізований та

введений в дію єдиний для всіх користувачів порядок надання, зміни та скасування доступу до ІзОД у відповідності до встановлених політик, який є обов'язковим для виконання всіма без виключення користувачами (сюди відноситься і весь топ-менеджмент підприємства без будь якого виключення).

Нижче наведено базові складові, що рекомендується включати в політику категорування ІзОД. Ці складові формалізовано на основі практичного досвіду впровадження DLP та DAG систем, а також на реальному прикладі продемонструвати один із варіантів підходу щодо забезпечення безпеки інформаційних активів, що беруть участь в бізнес-процесах підприємства, і можуть бути використані про розгортанні DLP та DAG систем (система запобігання витокам інформації та система управління доступом до неструктурованих даних) для захисту ІзОД.

Рекомендації спрямовані на забезпечення проведення наступних робіт:

- формування реєстру інформаційних активів;
- формування системи управління інформаційними активами;
- розгортання системи управління доступом до неструктурованих даних;
- розгортання системи протидії витокам інформації.

Зрозуміло, що у роботах з категорування інформаційних активів і забезпечення управління ними повинні брати участь усі керівники структурних підрозділів або особи, уповноважені ними, співробітники підрозділів ІТ-адміністратори сховищ, на яких розміщуються інформаційні активи, а також фахівці з ІБ. В процесі виконання рекомендацій повинен бути визначений структурний підрозділ, який буде управляти і є власником перерахованих нижче процесів. Як правило, це служба інформаційної безпеки (СлІБ).

Терміни та визначення. Для однозначного трактування термінів, що використанні при розробці політики категорування інформації, їх визначення наведено в табл. 1.

Таблиця 1

Терміни та визначення

Термін	Визначення
Інформаційний актив	Матеріальний або нематеріальний об'єкт, який: є інформацією або містить інформацію, служить для обробки, зберігання або передачі інформації, має цінність для підприємства.
Інформація з обмеженим доступом (ІзОД)	Відомості підприємства про осіб, предмети, факти, події, явища і процеси, незалежно від форми їх подання, що є конфіденційною інформацією, комерційною таємницею, персональними даними, даними для внутрішнього користування або іншими відомостями, які охороняються відповідно до чинного законодавства України, а також нормативними актами і регламентуючими документами підприємства.
Підрозділ	Відокремлений підрозділ, субхолдинг, акціонерне товариство, компанія, завод, представництво, департамент, управління, відділ, служба чи інша організаційна одиниця, що розробляє конфіденційний документ або курирує його розробку силами сторонньої підприємства.
Керівники підрозділів	Керівники відокремлених підрозділів, субхолдингів, акціонерних товариств, заводів, філій, департаментів, управлінь, служб, відділів чи інших організаційних одиниць, а також їх заступники.
Комерційна таємниця	Інформація з обмеженим доступом, що дозволяє її власникові при існуючих або можливих обставин збільшити доходи, уникнути невиправданих витрат, зберегти положення на ринку товарів, робіт, послуг або отримати іншу комерційну вигоду.
Інформація, що становить комерційну таємницю	Науково-технічна, технологічна, інвестиційна, виробнича, фінансово-економічна або інша інформація (в тому числі складова секретів виробництва (ноу-хау), яка має дійсну або потенційну комерційну цінність в силу невідомості її третім особам, до якої немає вільного доступу на законній підставі й у відношенні якої власником такої інформації введений режим обмеженого доступу до інформації.
Захист інформації	Діяльність щодо запобігання витоку інформації, що захищається, а також несанкціонованих і ненавмисних дій на інформацію, що захищається.
Режим обмеженого доступу до інформації	Правові, організаційні, технічні та інші заходи, які приймаються власником відомостей, що становлять інформацію з обмеженим доступом, з охорони їх конфіденційності.
Категорія ІзОД	Застосовувані класи відомостей підприємства для Категорування інформації за ступенем обмеження доступу.
Категорія ІзОД: строго конфіденційно (СК)	Клас відомостей підприємства, що становлять конфіденційну інформацію зі строго регламентованим доступом і захистом – строго конфіденційна інформація.
Категорія ІзОД: комерційна таємниця (КТ)	Клас відомостей підприємства, що становлять комерційну таємницю.
Категорія ІзОД: персональні дані (ПДн)	Клас відомостей підприємства, що становлять персональні дані співробітників.
Категорія ІзОД: для службового (внутрішнього) користування (ДСК)	Клас відомостей підприємства, що містять інші відомості, які власник відносить до інформації з обмеженим доступом - для службового користування.
Категорія ІзОД: публічна (ПБ)	Клас відомостей підприємства, що не містять інформацію з відкритим доступом - публічна інформація.
Гриф ІзОД	Застосовувані обмежувальні грифи для маркування інформації на підприємстві за ступенем обмеження доступу: СК, КТ, ПДн, ДСК, ПБ (див. категорії ІзОД).

Виклад основного матеріалу дослідження

Зважаючи на ріст рівня інформаційних та кібернетичних загроз для підприємств різних форм власності, варто виокремити декілька основних тверджень щодо підходу до політики категорування ІзОД.

Твердження 1. Формування реєстру інформаційних активів

Для формування реєстру інформаційних активів необхідно визначити:

- перелік інформаційних активів, що обробляються кожним підрозділом, і провести їх категорування (визначити категорію ІзОД);
- перелік ІС, в яких обробляються та зберігаються інформаційні активи;
- перелік місць зберігання носіїв, що містять інформаційні активи (електронні та паперові);
- власника інформаційного активу та перелік підрозділів, доступ яким необхідний до активу для виконання співробітниками службових обов'язків.

Прикладами інформаційних активів можуть бути: договір з клієнтами, фінансова звітність, технологічна карта, журнал реєстрації листів, проекти нових продуктів або послуг, ноутбук з інформацією про фінансовий стан підприємства, сервер з інформацією про клієнтів, архів (приміщення) з паперовими справами співробітників підприємства, планшет керівника підприємства з планом перспективної та оперативної діяльності.

Інформаційні активи володіють основними властивостями фінансових та матеріальних активів підприємства: вартість, вартість для підприємства, можливість накопичення, можливість трансформації в інші активи. Дуже часто цінність інформаційного активу підприємства може перевершувати цінність всіх фінансових активів. Прикладом такого активу може бути імідж підприємства. Формування реєстру здійснюється шляхом отримання інформації від керівників структурних підрозділів, що обробляють інформаційні активи. При цьому керівники структурних підрозділів або уповноважені ним особи повинні надавати інформацію про всі види інформаційних активів, що отримуються, створюються і передаються в ході реалізації бізнес-процесів співробітниками їх підрозділів.

Твердження 2. Інформаційне наповнення реєстру

Реєстр повинен містити наступну інформацію:

1) назва інформаційного активу;

2) місце обробки інформаційного активу (інформаційна система, називання БД, файловий ресурс, обробка в паперовому вигляді і т.д.);

3) критичність інформаційного активу – конфіденційність, цілісність, доступність;

4) опис активу – характеристика оброблюваної інформації, опис типових форм і документів (наприклад, картка Т2, форма договору, анкета);

5) термін зберігання інформаційного активу;

6) доступ до інформаційного активу – перелік ролей і їх прав.

Примітка – будь-які додаткові відомості про інформаційні активи (порядок отримання активу, порядок передачі всередині підприємства, передаються чи активи третім особам і т.д.).

На першому етапі, для спрощення процедури збору інформації про інформаційні активи пропонується розробити СлІБ та впровадити на підприємстві типові форми опитування. При цьому до керівника структурного підрозділу повинно бути доведено, що він буде власником даного інформаційного активу і він відповідає за правильне категорування інформації щодо даного інформаційного активу. Надалі, надання доступу до інформаційного активу в обов'язковому порядку повинно узгоджуватися з його власником.

За результатами отримання інформації від керівників структурних підрозділів представляється можливим заповнити частину граф реєстру інформаційних активів. Надалі керівники структурних підрозділів, на підставі затвердженого «Переліку відомостей підприємства, що становить інформацію з обмеженим доступом», визначають або уточнюють для кожного інформаційного активу його категорію. Ми будемо розглядати п’ять типових класів активів для підприємства, як найбільш типовий перелік при впровадженні DLP систем: публічна інформація, інформація для внутрішнього (службового) користування, персональні дані, комерційна таємниця, суворо конфіденційна інформація (див. як приклад табл. 2).

Зрозуміло, що даний перелік не може претендувати на повноту охвату всього існуючого переліку інформації з обмеженим доступом на кожному підприємстві, але він може бути базовим для формування політики категорування ІзОД і для кожного підприємства цей перелік повинен бути сформований з врахуванням його особливостей обробки і зберігання ІзОД. Результати класифікації вписуються в реєстр інформаційних активів. Реєстр інформаційних активів доцільно вести в електронному вигляді що спрощує його підтримку в актуальному стані, а також дозволяє використовувати відповідні автоматизовані системи його ведення. Також повинні бути визначені власник, місце зберігання і обов'язки з ведення реєстру інформаційних активів.

Твердження 3. Управління інформаційними активами

Для забезпечення безпеки інформаційних активів необхідно документувати і впровадити такі процеси:

1) надання доступу до інформаційних активів;

2) забезпечення безпеки носіїв;

3) структурування інформаційних активів у сховищах;

Таблиця 2

Приклад переліку відомостей підприємства, що становлять інформацію з обмеженим доступом

А1. СУВОРО КОНФІДЕНЦІЙНІ ВІДОМОСТІ

А1.1. Відомості про структуру підприємства та її власників

№	Перелік відомостей	Гриф
1	Відомості про корпоративну структуру підприємства.	СК
2	Відомості про бенефіціарів (справжніх власників, вигодонабувачів) в частині, що не підлягають розголошенню відповідно до діючого законодавства.	СК
3	Відомості про плани зміни структури акціонерного капіталу.	СК
4	Відомості про угоди, що готуються з придбання або поглинання активів.	СК
5	Інформація, підготовлена для власника(ів) і керівництва підприємства.	СК
6	Матеріали, пов'язані з діяльністю органів управління і контролю.	СК
7	Матеріали, пов'язані з підготовкою до проведення засідань і загальних зборів органів управління і контролю державного або приватного секторів до факту їх публічного розкриття в офіційних документах.	СК
8	Інформація про нарадах, ділових зустрічах, запланованих заходах.	СК
9	Відомості про прийняті рішення, щодо змін (вдосконалення) корпоративної структури, включаючи ліквідації, створення, придбання, злиття, поглинання, перетворення, створення філій, представництв, участі в різних об'єднаннях, зміни складів наглядових рад, зміни ключових посадових осіб (топ-менеджерів, директорів напрямків).	СК
10	Відомості про зміни статутного капіталу, або що планується чи вже йде скуповування пакетів акцій або часток інших підприємств.	СК
11	Плани та юридична позиція по вирішенню господарських, в тому числі податкових, суперечок (як наявних, так і можливих), трудових спорів, позицій з досудового врегулювання до факту їх розкриття в документах, офіційно подаються за обраною процедурою оскарження.	СК
… n	Відомості ….	СК

А1.2. Відомості щодо забезпечення загальної безпеки

№	Перелік відомостей	Гриф
1	Відомості про діяльність, структуру, штат управління з питань безпеки та служби інформаційної безпеки.	СК
2	Відомості, що розкривають об'єкти зацікавленості управління з питань безпеки та служби інформаційної безпеки.	СК
3	Відомості, що розкривають суть службових розслідувань і перевірок управління з питань безпеки та служби інформаційної безпеки.	СК
4	Аналітичні довідки і звіти за результатами роботи управління з питань безпеки та служби інформаційної безпеки.	СК
… n	Відомості, що ...	СК

А2. ВІДОМОСТІ, ЩО СКЛАДАЮТЬ КОМЕРЦІЙНУ ТАЄМНИЦЮ

А2.1. Відомості фінансового і економічного характеру

№	Перелік відомостей	Гриф
1	Відомості, що розкривають порядок і строки забезпечення фінансовими засобами.	КТ
2	Відомості, що містяться в регістрах бухгалтерського обліку, бухгалтерські звіти (крім тих, які опубліковані).	КТ
3	Відомості, що розкривають в цілому бюджетні показники або зведену фінансову звітність за структурними підрозділами державного або приватного секторів.	КТ
4	Відомості, що розкривають асигнування, фактичні витрати	КТ
	і кредитну заборгованість державного або приватного секторів.	КТ
5	Відомості про фінансові взаємини зі співробітниками, в тому числі відомості про заробітну плату, премії та витрати співробітників.	КТ
6	Відомості про інвестиційні операції, короткострокових і довгострокових укладеннях, наданих позиках і гарантіях, боргових зобов'язаннях (регістри бухгалтерського обліку).	КТ
7	Відомості про залишки на рахунках в банках і інших кредитних організаціях і операції, які здійснює за цими рахунками.	КТ
8	Відомості, що стосуються політики державного або приватного секторів, в валютних і кредитних питаннях.	КТ
9	Відомості про політику в сфері ціноутворення, в тому числі про методи розрахунку, структуру, рівні цін на товари, роботи, послуги та про розміри знижок, що надаються конкретним споживачам.	КТ

Продовження табл. 2

10	Відомості, що містяться в регістрах бухгалтерського обліку, бухгалтерські звіти (крім тих, які опубліковані).	КТ
… n	Відомості, що ...	КТ

А2.2. Відомості про системи автоматизації, зв'язку і технічних засобах

№	Перелік відомостей	Гриф
1	Зведені відомості про використовувані засоби зв'язку та автоматизації, їх станом і плани щодо їх модернізації.	КТ
2	Відомості про результати інформаційних обстежень.	КТ
3	Відомості, що розкривають правила обробки інформації в інформаційних системах державного або приватного секторів, структуру інформаційних ресурсів державного або приватного секторів.	КТ
4	Відомості, що розкривають процес розробки програмного забезпечення, результати управлінських і технічних рішень.	КТ
5	Зведені відомості, що розкривають склад і параметри технічних засобів і зміст технічної документації виробів (устаткування).	КТ
6	Відомості, що розкривають вихідні дані, склад і зміст програмного забезпечення.	КТ
7	Відомості про алгоритми роботи і влаштуваннях інтерфейсу будь-якого ПЗ, систему та методи подання, організації та систематизації інформації в базах даних, вихідні коди програмного забезпечення.	КТ
8	Відомості, що відносяться до роботи криптографічного (шифрувальної) техніки або її частин, секретні ключі, паролі.	КТ
9	Відомості, що містяться в базах даних, що належать державного або приватного секторів та / або використовуються ним.	КТ
10	Відомості, що містяться в специфікаціях апаратного і програмного забезпечення, технічних описах, технічних завданнях на створення апаратного і програмного забезпечення, а також в іншій технічній та допоміжної документації.	КТ
… n	Відомості, що …	КТ

А2.3. Відомості що представляють собою «ноу-хау», стосуються технології виробництва продукції, проведення робіт і надання послуг

№	Перелік відомостей	Гриф
1	Відомості з технічних розробок і проектів, що містять оригінальні рішення (know-how).	КТ
2	Відомості про особливості технологій, що використовуються або пропонується прийняти, власних або придбаних, а також про специфіку їх застосування.	КТ
3	Відомості про програми перспективних досліджень і розробок, їх цілі та завдання.	КТ
4	Відомості про ключові ідеї і результати науково-дослідних розробок, в тому числі незавершених.	КТ
5	Відомості про умови експериментів і устаткуванні, на якому вони проводилися.	КТ
6	Відомості про особливості конструкторсько-технологічних рішень, що дають позитивний економічний ефект.	КТ
7	Відомості про сутність винаходів, корисних моделей і / або промислових зразків до офіційної публікації інформації про них.	КТ
… n	Відомості про ...	КТ

А2.4. Відомості по зовнішньої діяльності та взаємовідносинам

№	Перелік відомостей	Гриф
1	Відомості, що розкривають зміст матеріалів обстежень замовників, що включають інформацію з обмеженим доступом.	КТ
2	Відомості про застосовування оригінальних методів маркетингових досліджень, вивчення ринку і їх результати, про оцінки стану і перспективи розвитку ринкової кон'юнктури продажів	КТ
3	Відомості щодо стратегії освоєння ринку, в тому числі і інформація про застосовування оригінальних методів продаж.	КТ
4	Відомості, що розкривають структуру і зміст баз даних клієнтів (поточних і потенційних).	КТ
5	Зведені відомості по контактам з потенційними і поточними клієнтами і партнерами.	КТ
6	Відомості, про підготовку, хід та результати переговорів з третіми особами.	КТ
7	Відомості, що розкривають зміст комерційних пропозицій клієнтам, в тому числі конкурсних пропозицій.	КТ
8	Конфіденційні відомості, які стали відомі в зв'язку з виконанням зобов'язань за договорами з третіми особами, в тому числі пов'язані з комерційною та іншою захищеною законом таємницею контрагентів.	КТ

Продовження табл. 2

9	Зведені відомості про вартість закупленої продукції, терміни і умови поставок.	КТ
… n	Відомості, що …	

А2.5. Відомості про виробничі процеси

№	Перелік відомостей	Гриф
1	Відомості, що розкривають зміст внутрішніх стандартів підприємства.	КТ
2	Відомості про результати внутрішніх перевірок та звіти про стан виробництва.	КТ
3	Відомості з управління якістю.	КТ
4	Відомості про плани залучення постачальників і підрядників, а також відомості про техніко-економічне обгрунтуваннях таких планів.	КТ
5	Відомості про інвестиційні плани і техніко-економічне обгрунтуваннях таких планів.	КТ
6	Відомості про плани розширення або згортання виробництва, різних видів продукції (реалізації товарів, виконання робіт, надання послуг і т.п.), а також відомості про техніко-економічне обгрунтуваннях таких планів.	КТ
… n	Відомості про …	КТ

А3. ВІДОМОСТІ ДЛЯ СЛУЖБОВОГО КОРИСТУВАННЯ

А3.1. Відомості з організаційно-штатних питань

№	Перелік відомостей	Гриф
1	Відомості, що стосуються допуску до конфіденційної інформації працівників.	ДСК
2	Відомості про плинність кадрів, напрямки кадрової політики керівництва..	ДСК
3	Відомості, що містять персональні дані працівників і підлягають захисту відповідно до діючого законодавства, а також інша персональна інформація.	ПДн
… n	Відомості щодо …	ПДн

А3.2. Відомості про виробничі процеси

№	Перелік відомостей	Гриф
1	Відомості про порядок організації технологічних процесів виробництва продукції, а також відомості про затверджену номенклатурі, обсяг і якість продукції.	ДСК
2	Відомості про порядок формування виробничих програм, нормативів витрачання сировини, матеріалів та енергоресурсів.	ДСК
3	Відомості про порядок організації та забезпечення екологічної безпеки виробничої / господарської діяльності.	ДСК
4	Відомості про порядок організації капітальних і поточних ремонтів обладнання, робіт з утримання будинків і споруд, робіт з модернізації та реконструкції обладнання, а також міжремонтного обслуговування.	ДСК
5	Відомості про порядок формування і розрахунки нормативів витрат сировини і товарно-матеріальних цінностей на всі види виконуваних робіт.	ДСК
6	Відомості про порядок організації та забезпечення розробок проектно-кошторисної та конструкторської документації, технічної документації для формування реєстраційних профілів та супровідної документації.	ДСК
7	Відомості про порядок організації технологічних процесів виробництва продукції, а також відомості про затверджену номенклатурі, обсяг і якість продукції.	ДСК
8	Відомості про порядок формування виробничих програм, нормативів витрачання сировини, матеріалів та енергоресурсів.	ДСК
… n	Відомості про …	ДСК

А3.3. Відомості про забезпечення охорони об'єктів

№	Перелік відомостей	Гриф
1	Відомості, що розкривають склад технічних систем охорони об'єктів підприємства, організаційні заходи щодо системи охорони об’єктів.	ДСК
2	Відомості, що розкривають порядок пропускного режиму на об'єкти підприємства, заходи, що його забезпечують.	ДСК
3	Відомості, що розкривають структуру і функції чергових змін охорони.	ДСК
4	Інструкції служби фізичної та інформаційної безпеки.	ДСК
… n	Відомості щодо …	ДСК

Закінчення табл. 2

А3.4. Відомості щодо забезпечення інформаційної безпеки

№	Перелік відомостей	Гриф
1	Відомості про застосовувані системи і засоби захисту інформації на підприємстві, а також зміст заходів щодо забезпечення інформаційної та кібернетичної безпеки автоматизованих систем обробки інформації, автоматизованих систем управління виробництвом, систем зв'язку та т.п.	ДСК
2	Відомості про грубі порушення вимог інформаційної та кібернетичної безпеки.	ДСК
3	Відомості про потреби, призначення, наявність, каналів руху ключових документів, про склад ключових мереж, що плануються до розгортання і діючих, факти компрометації і відновлення, ін.	ДСК
4	Відомості, що стосуються ключових інформаційних систем.	ДСК
5	Відомості про результати контролю переговорів по відкритих каналах зв'язку.	ДСК
6	Відомості про технічні засоби перехоплення, знімання інформації, та методи їх застосування.	ДСК
7	Відомості, що розкривають значення діючих кодів, паролів, які використовуються для підтвердження повноважень при встановленні зв'язку і доступу до інформаційних систем підприємства.	ДСК
8	Відомості, що розкривають питання організації робіт і стан інформаційної безпеки, сутність заходів щодо забезпечення інформаційної та кібернетичної безпеки, режиму конфіденційності.	ДСК
9	Відомості, що розкривають результати досліджень з виявлення каналів витоку конфіденційної інформації на підприємстві.	ДСК
10	Відомості про методи захисту від підробки зображень, що відтворюють товарні знаки та інші засоби індивідуалізації підприємства, його продукції, робіт і послуг.	ДСК
11	Політики та інструкції служби інформаційної безпеки.	ДСК
12	Політики та інструкції управління інформаційних технологій.	ДСК
… n	Відомості про …	ДСК

4) повідомлення працівників про правила використання корпоративних ресурсів;

5) контроль за дотриманням вимог розміщення інформаційних активів.

Твердження 4. Надання доступу до інформаційних активів

Для управління доступом до інформаційних активів доцільно розробити та використовувати рольову модель користувача, яка повинна включати в себе структуру прав доступу до відповідних інформаційних активів.

Надання доступу до інформаційних активів доцільно здійснювати за заявкою від керівника підрозділу, якому належить співробітник з обов'язковим погодженням доступу з власником інформаційного активу і СлІБ. Надання доступу має ґрунтуватися на принципі «need to know», тобто співробітники повинні мати доступ тільки до тих активів (даними), які необхідні їм для виконання їх посадових обов'язків, і вони (співробітники) повинні володіти мінімально необхідними привілеями.

Оригінали узгоджених заявок повинні зберігатися в управлінні інформаційних технологій (УІТ). Копії погоджених заявок повинні передаватися в електронному вигляді в СлІБ.

Періодично необхідно проводити інвентаризацію облікових записів, що підтверджує, що:

1) для всіх активних облікових записів існують узгоджені заявки;

2) усі облікові записи звільнених співробітників заблоковані;

3) неперсоніфіковані, колективні, групові облікові записи не використовуються для цілей адміністрування;

4) всі тестові облікові записи активні тільки на час проведення робіт.

Результати інвентаризації повинні оформлятися у вигляді акту, що описує результати перевірки.

Всі знайдені невідповідності реальних прав доступу наявними заявками повинні бути усунені.

Твердження 5. Забезпечення безпеки носіїв

Носії інформаційних активів необхідно захищати. Для цього доцільно:

1) промаркувати носії інформації;

2) регулярно проводити інвентаризацію носіїв інформації;

3) забезпечити їх фізичну безпеку;

4) визначити порядок доступу до носіїв інформації.

Носії інформації рекомендується промаркувати наклейками, що містять обліковий номер і найменування класу активу. При цьому носії інформації доцільно враховувати у відповідних журналах і проводити регулярну інвентаризацію носіїв (рекомендується проводити інвентаризацію не менше, ніж раз на рік).

Для забезпечення фізичної безпеки носіїв інформаційних активів рекомендується обмежити доступ в приміщення, де здійснюється їх обробка та збері-

гання. Носії, на яких зберігається і / або обробляється суворо конфіденційні відомості, комерційна таємниця або інформація для внутрішнього користування, доцільно зберігати в приміщеннях, обладнаних системою контролю доступу. Матеріальні носії доцільно зберігати в сейфах або шафах, що замикаються. Порядок забезпечення різних аспектів фізичної безпеки носіїв, які використовуються для зберігання та обробки ІзОД, повинні бути визначені додатковими процедурами та інструкціями.

Доступ до носіїв, які містять інформаційні активи, необхідно надавати відповідно з виробничою необхідністю, в рамках виконання співробітниками своїх посадових обов'язків.

Твердження 6. Структурування інформаційних активів на файлових ресурсах

Пропонується упорядкувати інформаційні активи, що розміщуються у сховищах різного типу.

Для цього УІТ з урахуванням інформації, документованої в реєстрі інформаційних активів, формує архітектуру каталогів. Спрощена структура каталогів може бути представлена у вигляді поданому на рис. 1.

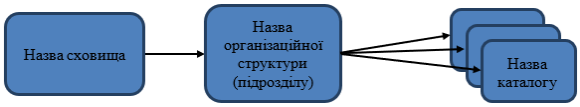

Рис. 1. Пропонована структура каталогів

ІТ фахівці – адміністратори сховищ, формують нову структуру каталогів і розмежовують права доступу до нових папок відповідно до реєстру інформаційних активів. ІТ фахівці також визначають максимальний розмір дискового простору каталогів верхнього рівня.

Після завершення процесу створення структури каталогів, керівники структурних підрозділів або уповноважені особи все дані, що зберігаються на корпоративних ресурсах, переглядають і переносять (копіюють) їх відповідно до визначених каталогів. При цьому всіх користувачів інформаційних ресурсів необхідно повідомити про процес перенесення даних і представити їм опис нової структури та інструкції щодо порядку обробки та зберігання інформаційних активів підприємства.

Після цього рекомендується впровадження автоматизованих систем інтелектуального аналізу сховищ даних, використання яких дозволяє підвищити ефективність управління доступом і зберігання ІзОД підприємства.

Твердження 7. Повідомлення працівників про правила використання корпоративних ресурсів

Пропонується по захищеній електронній пошті або через захищений корпоративний веб-ресурс провести розсилку внутрішнім адресатам інструктивних матеріалів з визначенням вимог щодо розміщення інформаційних ресурсів підприємства на корпоративних ресурсах. Вимоги щодо розміщення інформаційних активів пропонується оформити окремим документом – «Правила розміщення інформаційних активів на корпоративних ресурсах».

До складу правил пропонується включити:

вимоги щодо необхідності зберігання документів тільки відповідно до прийнятої структури;

перелік категорій інформації, доступної для розміщення на корпоративних ресурсах (наприклад, документи, призначені для роботи);

перелік інформації, розміщення якої заборонено на корпоративних ресурсах (наприклад, інформація особистого характеру, відеофільми, фотографії та ін.);

вимога своєчасно видаляти інформацію, яка не потрібна для виконання бізнес-процесів і цілі обробки якої, досягнуті.

Будь-яку іншу інформацію, що стосується підвищення корпоративної культури роботи з сховищами даних. У внутрішні документи підприємства доцільно прописати відповідальність працівників за дотримання поточних вимог.

Твердження 8. Контроль за дотриманням вимог розміщення інформаційних активів

Контроль за дотриманням вимог щодо розміщення інформаційних активів здійснюють власники інформаційних активів. З періодичністю не рідше одного разу на півроку-рік власник інформаційного активу повинен переглядати дані в каталогах на предмет виконання вимог щодо їх розміщення.

Висновки

Питання організації безпеки інформації з обмеженим доступом, а зокрема управління зберіганням та наданням прав доступу до неї, на даний час досить гостро стоїть у цілому світі. Особливо це актуально для підприємств, що починають впроваджувати автоматизовані DLP та DAG системи. Проаналізовані і сформовані рекомендації та вимоги щодо розробки політики категорування ІзОД щодо ІР підприємств різних форм власності. Звернута увага на прикладні аспекти що можуть допомогти суттєво зменшити ризики пов’язані з НСД до ІзОД, знищенням інформаційних ресурсів, компрометації ІР підприємства і т.п. Подальші дослідження варто зосередити на створенні та впровадженні типового положення про ІзОД та порядку захисту інформаційних активів підприємств державного та корпоративного сектору економіки, розробці та імплементації сучасних методик та стандартів протидії інформаційним та кібернетичним загрозам, навчанні та тренінгам персоналу правилам класифікації та категоруванню інформації.

Список літератури

1. Управління доступом. TechNet – Microsoft. – [Електронний ресурс]. – Режим доступу до ресурсу: https://technet.microsoft.com/ru-ru/library/cc770749(v=ws.11).aspx.

2. Рольове управління доступом для IBM Systems Director Console. – [Електронний ресурс]. – Режим доступу до ресурсу: http://www.ibm.com/support/knowledgecenter/ru/ssw_aix_71/com.ibm.aix.sysdircon/rbac_main.htm.

3. Левкин Р. Внедрение DLP-системы на предприятии / Р. Левкин. – [Електронний ресурс]. – Режим доступу до ресурсу: https://www.anti-malware.ru/analytics/Technology_Analysis/introduction_DLP_system_enterprise.

4. Защита от потери данных – Microsoft. – [Електронний ресурс]. – Режим доступу до ресурсу: https://technet.microsoft.com/ru-ru/library/jj150527(v=exchg.150).aspx.

5. Хмелин А. Практические аспекты внедрения системы защиты от утечек даннях / А. Хмелин. – [Електронний ресурс]. – Режим доступу до ресурсу: http://www.s-director.ru/magazine/magdocs/view/129.html.

6. Бурячок В.Л. Сучасні системи виявлення атак в інформаційно-телекомунікаційних системах і мережах. Модель вибору раціонального варіанта реагування на прояви стороннього кібернетичного впливу / В.Л. Бурячок // Інформаційна безпека. Східноукраїнський національний університет ім. В.Даля. – 2013. – № 1(9). – С. 33-40.

7. Бурячок В.Л. Політика інформаційної безпеки: підручник / В.Л. Бурячок, Р.В. Грищук, В.О. Хорошко. – К.: ПВП «Задруга», 2014. – 222 с.

8. Бурячок В.Л. Сучасні методи комплексної оцінки ефективності захисту інформації в розподілених корпоративних мережах / В.Л. Бурячок, В.А. Козачок // Матеріали міжнародної науково-технічної конференції «Сучасні інформаційно-телекомунікаційні технології». – Том 4: Сучасні технології інформаційної безпеки. – ДУТ, С. 91-92.

9. Бурячок В.Л. Пентестінг як інструмент комплексної оцінки ефективності захисту інформації в розподілених корпоративних мережах / В.Л. Бурячок, В.А. Козачок, Л.В. Бурячок, П.М. Складанний // Сучасний захист інформації. – Державний університет телекомунікацій. – 2015. – № 3. – С. 4-12.

10. Бурячок В.Л. Науково-технічне обґрунтування вибору підходу до формування множини інформативних параметрів для систем захисту інформації / В.Л. Бурячок, Р.В. Грищук, В.М. Мамарєв // Специальные телекоммуникационные системы и защита информации. – 2014. – № 2(26). – С. 82-86.

11. Бурячок В.Л. Технологія проведення порівняльного аналізу та оцінювання стану захищеності автоматизованих інформаційних систем / В.Л. Бурячок, Л.В. Бурячок, В.В. Семко // Сучасний захист інформації. – Державний університет телекомунікацій. – 2016. – № 4. – С. 16-24.

References

1. TechNet-Microsoft, *Access control*, https://technet.microsoft.com/en-us/library/cc770749(v=ws.11).aspx.

2. *Role-based access control for IBM Systems Director Console*, www.ibm.com/support/knowledgecenter/en/ssw_aix_71/com.ibm.aix.sysdircon/rbac_main.htm.

3. Levkin, R. *Implementation of the DLP system at the enterprise*, https://www.anti-malware.ru/analytics/Technology_Analysis/introduction_DLP_system_enterprise.

4. Microsoft, *Data loss protection*, https://technet.microsoft.com/en-us/library/jj150527(v=exchg.150).aspx.

5. Khmelin, A. *Practical aspects of implementation of the system of protection against data leaks*, www.s-director.ru/magazine/magdocs/view/129.html.

6. Buryachok, V. (2013), "Suchasni systemy vyiavlennia atak v informatsiino-telekomunikatsiinykh systemakh i merezhakh. Model vyboru ratsionalnoho varianta reahuvannia na proiavy storonnoho kibernetychnoho vplyvu" [Modern systems for detecting attacks in information and telecommunication systems and networks. A model for choosing a rational version of the response to manifestations of third-party cybernetic effects], *Information security*, No. 1 (9), Eastern Ukrainian National University V. Dahl, pp. 33-40.

7. Buryachok, V., Grischuk, R. and Khoroshko, V. (2014), "*Polityka informatsiinoi bezpeky: pidruchnyk*" [*Information security policy: a textbook*], PVP "Zadruga", Kyiv, 222 p.

8. Buryachok, V.L. and Kozachok, V.A., "Suchasni metody kompleksnoi otsinky efektyvnosti zakhystu informatsii v rozpodilenykh korporatyvnykh merezhakh" [Modern methods of integrated assessment of the effectiveness of information security in distributed corporate networks], *Materials of the international scientific and technical conference "Modern information and telecommunication technologies"*, Vol. 4, Modern technologies of information security, DUT, pp. 91-92.

9. Buryachok, V.L., Kozachok, V.A., Buryachok, L.V. and Skladannyi, P.M. (2015), "Pentestinh yak instrument kompleksnoi otsinky efektyvnosti zakhystu informatsii v rozpodilenykh korporatyvnykh merezhakh" [Pentesting as a tool of complex assessment of the effectiveness of information security in distributed corporate networks], *Modern information technology*, No. 3, State University of Telecommunications, pp. 4-12.

10. Buryachok, V.L., Grishchuk, R.V. and Mamarev, V.M. (2014), "Naukovo-tekhnichne obgruntuvannia vyboru pidkhodu do formuvannia mnozhyny informatyvnykh parametriv dlia system zakhystu informatsii" [Scientific and technical substantiation of the choice of approach to the formation of a set of informative parameters for information security systems], *Special telecommunication systems and information protection*, No. 2(26), pp. 82-86.

11. Buryachok, V.L., Buryachok, L.V. and Semko, V.V. (2016), "Tekhnolohiia provedennia porivnialnoho analizu ta otsiniuvannia stanu zakhyshchenosti avtomatyzovanykh informatsiinykh system" [Technology of conducting comparative analysis and evaluation of the state of protection of automated information systems], *Modern information protection*, No. 4, State University of Telecommunications, pp. 16-24.

Надійшла до редколегії 16.05.2018
Схвалена до друку 19.06.2018

Відомості про авторів:

Борсуковський Юрій Володимирович
кандидат технічних наук
доцент Державного університету телкомунікацій,
Київ, Україна
https://orcid.org/0000-0003-1973-2386

Борсуковька Вікторія Юріївна
ПАТ «Укрсоцбанк» департамент безпеки
керівник проектів,
Київ, Україна
https://orcid.org/0000-0002-4929-6987

Бурячок Володимир Леонідович
доктор техніних наук професор
завідуючий кафедрою
Київського університету ім. Б. Грінченка,
Київ, Україна
https://orcid.org/0000-0002-4055-1494

Скаладанний Павло Миколайович
старший викладач Київського університету
ім. Б. Грінченка,
Київ, Україна
https://orcid.org/0000-0002-7775-6039

Information about the authors:

Yurii Borsukovskii
Ph.D. in Technical Sciences
Senior Lecturer of State University of Telecommunications,
Kyiv, Ukraine
https://orcid.org/0000-0003-1973-2386

Victoria Borsukovska
PJSC "Ukrsotsbank" Security Department
Kyiv, Ukraine,
https://orcid.org/0000-0002-4929-6987

Volodymyr Buriachok
Doctor of Technical Sciences Professor
Head of the Department of Borys Grinchenko
Kyiv University,
Kyiv, Ukraine
https://orcid.org/0000-0002-4055-1494

Pavlo Skladannyi
Senior Lecturer of
Borys Grinchenko Kyiv University,
Kyiv, Ukraine
https://orcid.org/0000-0002-7775-6039

ПРИКЛАДНЫЕ АСПЕКТЫ РАЗРАБОТКИ ПОЛИТИКИ КАТЕГОРИРОВАНИЯ ИНФОРМАЦИИ С ОГРАНИЧЕННЫМ ДОСТУПОМ

Ю.В. Борсуковский, В.Ю. Борсуковская, В.Л. Бурячок, П.М. Складанный

В статье проведен детальный анализ прикладных аспектов разработки политики информационной безопасности по категорированию информации с ограниченным доступом для корпоративных пользователей, которые начинают внедрять автоматизированные DLP и DAG системы. С учетом того, что в отечественном законодательстве четкое понимание понятия «коммерческая тайна» отсутствует, а каждый владелец предприятия может самостоятельно определять перечень информации, которая для него и предприятия в целом является конфиденциальной, а также самостоятельно определять порядок работы с такой информацией, в статье, во-первых, сформулированы базовые требования и рекомендации по структуре и содержанию типичной политики категорирования информации с ограниченным доступом для предприятий различных форм собственности, и, во-вторых, введен ряд новых понятий, которые позволят избежать конфликта при внедрении DLP и DAG систем с определенными их трактовками, определенными на законодательном уровне. Как результат, это приведет к существенному уменьшению рисков, связанных с несанкционированным доступом к конфиденциальной информации, уничтожением информационных ресурсов, компрометацией информационных ресурсов предприятия. Вместе с тем, в статье рассмотрен пример категорирования информации с ограниченным доступом; определены требования по формированию реестра информационных активов и сформированы рекомендации по категорированию информации с учетом опыта внедрения систем управления доступом к неструктурированным данным и систем предотвращения утечек информации.

Ключевые слова: *категорирование, классификация, доступ, политика, кибербезопасность.*

POLICY ASPECTS IN CRYPTO PROTECTION OF CONFIDENTIAL INFORMATION

Y. Borsukovskii, V. Borsukovska, V. Buriachok, P. Skladannyi

The article provides the detailed analysis for Information Security Poicies elaboration, considering categorization of restricted access information for corporate clients, which starts to implement automated DLP and DAG systems. However, the local legislation has no clear definition of "commercial secrecy", and each owner to the company may independently categorize the information which, in general, might be defined as confidential; as well define the procedure for operation with such type of information. Thus, the article covers: 1. Basic requirements for the structure and scope of model policy for restricted access information categories related to any type of legal entity. 2. Introduce the new definitions which ensure to avoid any conflicts in DLP and DAG systems implementation, considering its initial definition in legislation. In result, it will promote the essential decrease in risks related to illegal access to confidential information, damage of informational sources, and discredit of informational sources of the company. At that, the article provides the example of categorization in restricted access information; enlist the requirements for composition of information assets register and collects the practical recommendations for categorization of information considering the experience in implementation of access management systems to unstructured data and data security systems.

Keywords: *categorization, classification, access, politics, cyber security.*