предприятия (организации), а второй к сети интернет. В этом случае кабели собственной сети с защитой информации и кабели открытой сети интернет очень трудно разнести на достаточное расстояние. Вследствие этого информация, циркулирующая в локальной сети, а также все побочные излучения компьютеров, наведенные на кабели локальной сети, могут наводиться и на кабели открытой сети интернет. Мало того, что кабель открытой сети это достаточно длинная антенна (особенно когда открытая сеть проложена неэкранированным кабелем). Кабели открытой сети как правило выходят за границы охраняемой территории, поэтому снять информацию можно не только путем перехвата излучений, но и путем непосредственного подключения к кабелям открытой сети. Поэтому кабели открытой сети также должны быть проложены в соответствии со всеми рекомендациями, выполняемыми при построении сети с защитой информации.

Поступила 27.02.2003

УДК 681.3

Головань С.М., Давиденко А.М., Щербина В.П.

ВИБІР ОПТИМАЛЬНОГО ВАРІАНТУ КОНТРОЛЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ ТА ПЕРЕПУСКНОГО РЕЖИМУ

Одним із важливих заходів забезпечення захисту інформації з обмеженим доступом на підприємствах, в установах і організаціях є регулярний контроль. Але останнім часом відбувається значне збільшення обсягів контрольної інформації, що веде до збільшення витрат. Спробуємо розглянути цю проблему з точки зору необхідності, періодичності та якості контролю.

Контроль – перевірка, облік діяльності кого-, чого-небудь, нагляд за кимось, чимось [2].

Контроль здійснюється з метою оцінки дотримання законодавчих актів України, фактичного стану захисту інформації з обмеженим доступом, виявлення недоліків і порушень, встановлення їх причин, вироблення заходів спрямованих на усунення та попередження цих недоліків і порушень.

Контроль повинен мати системний характер і, як правило, він складається з двох частин. Перша – постійно здійснюється оперативний контроль за станом роботи підрозділу з захисту інформації з обмеженим доступом. Друга – періодично організується відповідно до заздалегідь складеного графіку перевірки за станом забезпеченням захисту інформації з обмеженим доступом.

Контроль поділяються на:

– комплексний, при проведенні якого всебічно перевіряється організація та стан захисту інформації з обмеженим доступом;

– цільовий, при проведенні якого перевіряються окремі питання діяльності та виконання вимог розпорядчих документів;

– перевірочний, коли перевіряється виконання пропозицій щодо виправлення помилок та усунення недоробок (за актами, довідками перевірки тощо).

Перевіряючий знайомиться з усіма документами, які мають відношення до питання, що перевіряється, а також проводить бесіди і консультації з фахівцями і виконавцями, при цьому необхідно використати такий обсяг матеріалу, який дозволив би зробити підсумок стану роботи в напрямку діяльності, що вивчався.

Задачі контролю:

- встановлення відповідності розпорядчих документів на підприємстві, в установі і організації законодавчим актам та розпорядчим документам України;
- вивчення та оцінка фактичного стану організації щодо забезпечення захисту інформації з обмеженим доступом на підприємстві, в установі і організації;
- виявлення порушень нормативних актів та помилок в організації захисту інформації з обмеженим доступом;
- встановлення причин недоробок і порушень та оцінку характеру кожної виявленої недоробки і порушення щодо можливості його привести до витоку інформації з обмеженим доступом як окремо так і разом з іншою інформацією;
- надання практичної допомоги в організації роботи по забезпеченню захисту інформації з обмеженим доступом;
- розробка положень та рекомендацій які сприятимуть усуненню і запобіганню недоробок, порушень;
- виявлення позитивного досвіду організації діяльності з метою його узагальнення та поширення;

Час контролю за станом забезпеченням захисту інформації з обмеженим доступом розбивається на періоди:

- підготовчий
- безпосередній контроль за станом забезпечення захисту інформації з обмеженим доступом;
- обробка і оформлення результатів контролю.

Елементами підготовчого періоду є вивчення стану забезпечення захисту інформації з обмеженим доступом, матеріалів попередніх перевірок.

Найпершою на цьому етапі є проблема вибору варіанту контролю. Параметрами оптимізації при цьому є обсяг та форма отримання контрольної інформації. Збирання надлишкової інформації веде до витрат часу перевіряючих, невдала форма або недостатність інформації веде до втрати якості контролю. Це в свою чергу веде до недоцільності здійснення контролю взагалі.

Використаємо методологію аналізу ризиків [1] у частині побудування таблиці контрольних запитань. А саме вивчення стану забезпечення захисту інформації з обмеженим доступом будемо проводити за допомогою опитувальної анкети, яка містить питання з усіх напрямків роботи підприємства, установи, організації які підлягають контролю і направляється та отримується заздалегідь (бажано за один або три місяці до початку запланованого контролю).

Розглянемо приклад формування опитувальної анкети стану забезпечення захисту інформації з обмеженим доступом підприємства, установи і організації.

При цьому повний перелік запитань оптимізується за вище згаданими параметрами, але не за рахунок повноти контролю. На підставі вивчення матеріалів розробляється перелік напрямків контрольно-перевірочної роботи.

Дата (число,місяць, рік)

Назва підприємства, установи, організації _____

Прізвище та ініціали керівника підрозділу захисту інформації з обмеженим доступом _____

Таблиця стану забезпечення захисту інформації з обмеженим доступом

/п	**Питання**	Так	Ні
	Чи виконані рекомендації та усунуті недоліки за підсумками всіх перевірок?		
	Чи відповідає штатна укомплектованість річній трудомісткості роботи підрозділу захисту інформації з обмеженим доступом?		
	Чи є положення про підрозділ захисту інформації з обмеженим доступом та чи повно викладені посадови обов'язки працівників?		
	Чи ведеться планування роботи підрозділу, що здійснює захист інформації з обмеженим доступом (перспективне, річне та квартальне) та є позначки про виконання?		
	Чи ведеться навчання і перевірка знань працівників та виконавців, вимог документів, що регламентують порядок роботи з матеріальними носіями інформації з обмеженим доступом?		
	Чи створені умови для роботи працівників та зберігання документів відповідають вимогами нормативних документів?		
	Чи ведеться контроль за правильність надання грифу обмеження доступу документам?		
	Чи ведеться контроль за нерозголошення відомостей, що містяться у документах з грифом обмеження доступу?		
	Чи ведеться перевірка знань співробітниками захисту інформації з обмеженим доступом інструкцій та дій на випадок пожежі, стихійного лиха, аварійних ситуацій тощо?		
0	Чи вірно ведеться приймання та реєстрація отриманих пакетів (конвертів) та документів?		
5	Чи вірно ведеться інвентарний облік документів?		
8	**Чи вірно ведеться розмноження документів з грифом обмеження доступу**		

Керівник підприємства Підпис Розшифровка підпису

Наприклад:

6. Створення умов для роботи працівників та зберігання документів з грифом обмеження доступу [3]:

- придатність та обладнання приміщень підрозділу згідно з вимогами нормативних документів;
- умови зберігання документів. Наявність шаф. Порядок зберігання дублікатів ключів від усіх сховищ для документів з грифом обмеження доступу;

- забезпечення збереження документів з грифом обмеження доступу при передачі їх між підрозділами, доповіді керівнику підприємства, установи і організації, доставці в інші підрозділи;

25. Інвентарний облік документів:

- організація робочого місця працівника, оргтехніка, меблі;
- реєстрація документів інвентарного обліку, відсутність підчисток та незавірених виправлень;
- зберігання, розмноження, відправка, знищення та передача документів інвентарного обліку в інші підрозділи;
- видача документів інвентарного обліку виконавцям;
- зберігання та знищення макулатури;
- оцінка ефективності та якості праці.

За результатами перевірки складається акт (довідка) з відображенням дотримання вимог законодавства, виявлені недоліки та порушення, пропозиції щодо їх усунення.

Невід'ємною складовою частиною захисту інформації з обмеженим доступом на підприємствах, в установах організаціях є дотримання пропускного та внутрішньооб'єктового режимів. В силу специфіки організації ця діяльність потребує особливого підходу до її контролю. Якість та результативність роботи щодо попередження витоку інформації з обмеженим доступом знаходяться в прямій залежності від знання та розуміння працівниками режимних вимог, дотримання пропускного та внутрішньооб'єктового режимів. В цьому випадку необхідно контролювати як теоретичну підготовку працівника так і його здібність зосереджувати увагу та мотивацію якісного виконання своїх службових обов'язків.

Пропускний режим – сукупність правил, що регламентують порядок входу (виходу) осіб, в'їзду (виїзду) транспортних засобів на територію підприємства, в установу і організацію, їх режимні території, зони або приміщення, занесення (винесення), завезення (вивезення) документів і виробів, а також заходів щодо реалізації цих правил.

В основі найбільш поширених і відносно недорогих пропускних систем, використовується принцип візуальної перевірки перепусток черговим на контрольно-пропускних пунктах або постів із пропускними функціями.

Перепустка – картка чи інший вид документа, виданий окремим особам, котрі працюють або котрим в силу інших причин потрібен санкціонований допуск на підприємство, в установу і організацію або на режимну територію, зону, приміщення з метою спрощення допуску та упізнання осіб, включаючи документи на транспортні засоби, видані для аналогічних цілей. Перепустками іноді називають посвідчення особи.

Враховуючи це на перепустках повинно бути чітко вказано основна інформація, необхідна працівнику контрольно-пропускного пункту або посту із пропускними функціями для встановлення особистості власника перепустки. Необхідно передбачити можливість щоб всі працівники, котрі працюють на режимній території, зоні, приміщенні на протязі всього робочого часу носили перепустку на видному місці верхнього одягу, з тим, щоб не виникла затримка при його візуальній перевірці.

На лицьовому боці перепустки повинен бути вміщена по крайній мірі наступна інформація:

- фотокартка працівника (власника). Для попередження користування перепусткою сторонньою особою. Чим більший розмір фотокартки, тим легше перевіряти її черговим контрольно-пропускного пункту або постом із пропускними функціями;
- прізвище працівника (власника). При необхідності його можливо звірити з іншими документами, такими як паспорт, посвідчення водія тощо;
- строк дії перепустки. При цьому необхідно чітко вказати цифрами місяць і рік закінчення строку дії, бажано чорнилами різного кольору, з тим щоб перешкодити використання прострочених перепусток і не рідше одного разу на рік необхідно проводити їх перевірку з метою встановлення їх справжності;

- режимну територію, зону, приміщення в котрі дозволено вхід працівнику (власнику перепустки);
- місце праці (орган державної влади, орган місцевого самоврядування, підприємство, установа, організація);
- серійний номер перепустки. Як і інформація про місце праці, ці данні необхідні для обліку перепусток працівниками підрозділу перепусток.

Крім цієї інформації, котру необхідно зазначати на кожній перепустці бажано унеможливити несанкціонований доступ за допомогою підроблення перепустки:

- встановити строк дії з регулярним обміном. Неминуче, що час від часу перепустки можуть бути загублені, крім того деякі працівники під час звільнення з роботи можуть не здати свої перепустки. Строк дії перепусток повинен не перевищувати двох років;
- кожен рік в разі заміни перепусток замінити колір заднього плану на фотокартці і розміщення даних;
- використання вдосконалених пластиків, котрі вступають в хімічну реакцію з матеріалом фотокартки, після чого її неможливо вилучити без пошкодження перепустки. Фотокартки можна також або запаяти в пластикову оболонку, бажано такого типу, щоб його розкриття привело до пошкодження фотокартки і перепустки;
- наносити знаки, виконані спеціальними засобами, котрі можливо бачити тільки під кутом.

При використанні електронної системи контролю на перепустку наноситься електронним пристроєм код, що зчитується.

Пропуск на режимну територію транспортних засобів повинен мати чимало з відмічених особливостей, передбачених для перепусток працівників, так як вони підлягають візуальної перевірки співробітниками контрольно – пропускних пунктів.

Наявність фірмового одягу само по собі не повинно розглядатися в якості належного і достатнього засобу посвідчення працівника.

Оформлення перепусток необхідно починати тільки після отримання письмової заявки з відповідним погодженням начальника підрозділу захисту інформації з обмеженим доступом або його заступника, який реально перевіряє, наскільки обґрунтована необхідність видачі такої перепустки. Такі заявки і заповнені перепустки повинні реєструватися. При отриманні перепустки її власник повинен поставити підпис за отримання в журналі видачі перепусток. Основним критерієм є те, наскільки часто даному працівнику необхідно працювати на режимній території, зоні чи приміщенні. При цьому в якості критерію прийняття рішення не може служити посада або службове положення.

Обмін перепусток необхідно проводити по графіку складеному з урахуванням кількості замінених перепусток так, щоб мати достатньо часу для вирішення адміністративно-виробничих питань та не допускати використання прострочених перепусток та контролювати, щоб перепустки не видавались працівникам, котрим доступ на режимну територію, зону, приміщення не потрібен чи потрібен в рідких випадках. При заміні великої кількості перепусток, доцільно використовувати річний цикл обміну, встановлюючи різні дати закінчення строку дії для різних підрозділів, що дає можливість рівномірно розподілити виробничу навантаження на протязі всього року (щоб визначити число перепусток які підлягають заміні в кожному місяці чи в кожному кварталі).

Внутрішньооб'єктового режим – організаційні та технічні заходи і правила щодо забезпечення режиму секретності, встановлені на підприємстві, в установі і організації.

Основними завданнями внутрішньооб'єктового режиму є:

- обмеження кола осіб, що допускаються до інформації з обмеженим доступом:
- проведення роботи з виконавцями щодо роз'яснення вимог роботи з документами, що мають гриф обмеження доступу та відповідальності за їх збереження;

– забезпечення встановленого порядку користування інформацією з обмеженим доступом.

Таким чином в даній роботі були розглянуті проблеми контролю стану забезпечення захисту інформації з обмеженим доступом, перепускного і внутрішньооб'єктового режиму та запропоновані підходи до його оптимізації.

Література:

1. Айков Д., Сейгер К., Фонсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. Пер. с англ. – М. – Мир. 1999. – 351 с.
2. Новий тлумачний словник української мови. У чотирьох томах. К., Аконіт. 1999 р.
3. Інструкція про порядок обігу, зберігання і використання документів, справ та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави. Затверджено постановою Кабінету Міністрів України від 27 листопада 1998 р., №1893 // Офіційний вісник України. – 1998. – № 48. – Ст. 1764.

Надійшла 28.02.2003

УДК 681.327

Федоренко Ю.І., Самохвалов Ю.Я.

ЗАХИСТ МАТЕРІАЛЬНИХ НОСІЇВ ІНФОРМАЦІЇ СПЕЦИФІЧНИМИ МІТКАМИ ТА ЇХ ЗЧИТУВАННЯ ШЛЯХОМ ВИКОРИСТАННЯ РАДІОІЗОТОПІВ

Специфічними мітками називаються мітки які встановлено на матеріальних носіях інформації, або предметах різними способами при:

– виготовленні;
– технологічному або спеціальному відхиленні, під час їх виготовлення;
– транспортуванні, використанні, зберіганні.

Такі мітки залишаються різними:

– технологічними лініями та інструментами;
– видами пломбіраторів та рельєфними печатками;
– видами вогнепальної зброї на снаряді, кулі, гільзі, шроту;
– ріжучими , колючими та іншими спеціальними інструментами та предметами, видами холодної зброї;
– вм'ятинами, подряпинами на матеріальних носіях інформації предметах культурно історичної спадщини держави;
– встановленими дрібними комплектуючими комп'ютерних систем (електронних плат та їх особливостей щодо мікроелементної бази, монтажу, часткове порушення фізичної цілісності струмопровідних доріжок тощо.) та інше.

Успішне застосування проходження (абсорбція) та відображення (зворотне розсіювання) β - випромінювання електронів все більше використовується у різних галузях промисловості.

Пропонується використовувати методи абсорбції та зворотного розсіяного β - випромінювання для зчитування та подальшої ідентифікації специфічних міток на матеріальних носіях інформації та предметах .

З метою визначення можливості застосування методу реєстрації зворотного розсіяного корпускулярного випромінювання для зчитування специфічних міток на пласких та круглих поверхнях і орієнтовної оцінки чутливості і погрішності були проведені експерименти на установці, схематично показаній на рис 2.1.