М.В. Рудик

Засоби попередження настання суспільно небезпечних наслідків від порушення правил експлуатації АЕОМ

На даному етапі розвитку людства, коли йде глобальна комп'ютеризація усіх виробничих процесів, персональні комп'ютери є вже практично у всіх установах та майже в кожному будинку. Їхні потенційні можливості величезні, вони відіграють роль робочих інструментів, використовуються для організації навчання, розваги й інших цілей. Однак, щоб комп'ютери справно працювали, за ними необхідний правильний догляд і дотримання правил експлуатації з боку обслуговуючого персоналу. Якщо ці правила не дотримуються, комп'ютери починають давати збої або просто виходять з ладу, у результаті чого можуть бути безповоротно змінені, знищені або навіть викрадені важливі дані, що являють собою, наприклад, банківську або комерційну таємницю. Наслідком даного порушення може бути заподіяння істотної шкоди охоронюваним законом інтересам, яка є безпосереднім результатом діяння винного.

Мета цієї статті – спроба вперше об’єднати технічні вимоги стосовно безпечної експлуатації АЕОМ з правовими нормами, які мають за мету захищати ці правовідносини, та на основі цього спробувати дати визначення правилам експлуатації автоматизованих електронно – обчислювальних машин.

У теорії кримінального права окремі проблеми захисту комп’ютерної інформації та кримінальної відповідальності за скоєння комп’ютерних злочинів досліджували такі відомі вчені, як П.І. Орлов, Ю.Кривонос, Д.Азаров, В.А. Терехов, О.І. Антонюк, Ю.Гульбін, В.С. Цимбалюк, В.О. Голубєв, Б.Завидов, Г.Л. Борисов, Д.А. Литваковський та інші. В їх дослідженнях дана лише загальна характеристика комп’ютерних злочинів, які передбачені ст.ст. 361, 362, 363 Особливої частини Кримінального кодексу України. Однак деякі питання і сьогодні залишаються дискусійними. Дуже мало уваги було приділено дослідженню такому важливому складу, як «Порушення правил експлуатації автоматизованих електронно-обчислювальних систем». Кримінальний кодекс України в ст. 363 передбачає відповідальність за порушення правил експлуатації автоматизованих електронно-обчислювальних систем. Однак законодавець не дає чіткого визначення таких правил, через що виникає питання, а що взагалі варто розуміти під правилами експлуатації автоматизованих електронно-обчислювальних систем? Перш за все, це суто технічні вимоги щодо догляду за комп'ютером, одночасно це і організаційно-правові норми, що мають за мету підпорядкувати та поставити під охорону важливі суспільні відносини, пов’язані з безпечним використанням комп’ютерної інформації в автоматизованих електронно-обчислювальних системах. Отож, під правилами експлуатації автоматизованих електронно-обчислювальних систем слід розуміти комплекс технічно-організаційних заходів правового напрямку, головною метою якого було б підтримання автоматизованих електронно-обчислювальних

систем в належному технічному стані, з одного боку, та протидія викраденню, перекрученню чи знищенню комп'ютерної інформації, засобів її захисту, або незаконному копіюванню комп'ютерної інформації, з іншого боку.

Також вважаємо за необхідне розробити чітку інструкцію для осіб, які відповідають за експлуатацію автоматизованих електронно-обчислювальних систем. Такою особою є користувач машин, а також інша особа, котра згідно зі своїми трудовими, службовими обов'язками або на основі відповідної угоди з власником ПОЕМ, виконує роботу, пов'язану з підтримкою останніх у робочому стані, і зобов'язана дотримуватись встановлених правил експлуатації, а також захисту інформації, що знаходиться в АЕОМ [1, с.907]. Що стосується технічних вимог, то їх необхідно знати, тому що інформація, яка міститься в комп'ютерах на сьогоднішній день піддається атакам з боку комп'ютерних вірусів та хакерів. Але це далеко не все. Перш за все необхідно пам'ятати, що нормальна робота вашого комп'ютера залежить від його чистоти. Так скупчення бруду, пилу, диму, можуть викликати необоротне перекручування, знищення комп'ютерної інформації або навіть спричинити повну відмову системи. Також періодичного чищення потребують дисководи для гнучких і для компакт-дисків, тому що їх забруднення відбувається досить часто. Недбале ставлення обслуговуючого персоналу може привести до погіршення якості читання і запису даних, а також до ушкодження самих носіїв або знищення комп'ютерної інформації, яка на них міститься. Поряд з пилом і брудом існує ще і такий, дуже пагубний для комп'ютерної інформації фактор, як температура. При експлуатації комп'ютера користувач рідко замислюється про клімат усередині комп'ютера. Система охолодження є одним з найважливіших компонентів будь-якого комп'ютера, від неї прямо залежить стійкість роботи ЕОМ і збереження відповідних комп'ютерних даних. Перевищення припустимого температурного режиму здатне істотно скоротити життя вашого комп'ютера, негативно позначитися на роботі комплектуючих і, навіть, вивести їх з ладу. Наприклад, особа, яка відповідає за експлуатацію АЕОМ, підключає до нього другий жорсткий диск, 3D прискорювач, інше додаткове устаткування, унаслідок чого зростає імовірність перегріву і, як результат недбалості щодо виконання експлуатаційних вимог з боку обслуговуючого персоналу – утрата важливої комп'ютерної інформації. Так, наприклад, перевищення припустимої температури на кожні 10 градусів здатне вдвічі скоротити термін служби основних компонентів ПК (найбільш комфортна температура усередині корпуса комп'ютера від 16 до 44 градусів C^0). Однак, якщо температура перевищить 55 градусів C^0 і більше, то може відбутися наступне: на підвищення температури дуже відчутно реагують жорсткі диски, передача інформації при цьому сповільнюється, збільшується імовірність її знищення.

Проте виконання перелічених вище експлуатаційних вимог з боку обслуговуючого персоналу не достатньо для безпечної роботи АЕОМ. Насамперед, необхідно пам'ятати, що безпечне і безперебійне електроживлення – запорука здорової роботи вашого ПК [2, с.13], а також надійний захист комп'ютерних даних від їх перекручування та знищення. Перепади і провали напруги в електромережі здатні зашкодити вашому комп'ютеру,

призвести до поломки вінчестера і, як наслідок, знищення всіх даних. У зв'язку з чим обслуговуючий персонал повинен дотримуватися наступних правил: 1) застосовувати мережні фільтри, 2) використовувати джерела безперебійного електроживлення. Важливо пам'ятати, що не слід ризикувати комп'ютером, ціна якого іноді доходить до 1000 доларів США, але інформація, яка на ньому може зберігатися, часом оцінюється мільйонами доларів США, у зв'язку з чим не слід заощаджувати коштів, необхідно придбати мережний фільтр і джерело безперебійного електроживлення.

Ми ще пам'ятаємо ті часи, коли відбувалися постійні відключення електроенергії, від яких страждали не тільки комп'ютери, але й інша побутова техніка. Так, при аварійному перериванні в електроживленні комп'ютер не в змозі коректно завершити роботу, та у процесі зчитування і запису інформації з жорсткого диска магнітні голівки знаходяться на відстані декількох мікронів від поверхні диска і надзвичайно важливо не допустити їх падіння на магнітну поверхню. Але коли електроживлення пропадає аварійно, голівки, що зчитують інформацію, можуть упасти на робочу поверхню жорсткого диска, що у свою чергу може спричинити механічне ушкодження поверхні жорсткого диска, а отже – безповоротну втрату інформації, що зберігається на «вінчестері».

Щоб цього не допустити, особам з кола обслуговуючого персоналу необхідно пам'ятати про користь джерел безперебійного живлення.

Навіть якщо строго дотримуватись перелічених вимог з експлуатації АЕОМ, ви рано або пізно можете зіткнутися з таким неприємним явищем, як викрадення комп'ютерної інформації. А якщо припустити, що під вашим підпорядкуванням знаходиться не один, не два комп'ютери, а десять і більше, то які прийоми і засоби слід застосувати, щоб попередити розкрадання настільки важливої комп'ютерної інформації? Як найбільш розумний варіант виходу з такої ситуації можна запропонувати наступний – це інтеграція проведеними вашою компанією програмами фізичного і технічного захисту територій і приміщень, а також розробка і впровадження спеціальних комп'ютерних програм, головною задачею яких було би попередження викрадення комп'ютерної інформації [3, с.181].

До технічних засобів захисту інформації можна віднести наступні: механічні, електронно-механічні, лазерні, радіолокаційні, акустичні, оптичні й інші пристрої, спорудження і системи, що покликані протистояти викраденню комп'ютерної інформації [4, с.35]. Так само необхідно відзначити, що територія повинна бути по можливості оточена забором, а периметр самого будинку повинний мати контрольовану зону. Спостереження ж за останньою може бути здійснене за допомогою різних телевізійних, лазерних, акустичних і інших систем, а також за допомогою систем датчиків, що підключені до центрального пульта охорони. Крім фізичних і технічних засобів захисту для забезпечення експлуатаційної безпеки, також важливі спеціальні комп'ютерні програми, що покликані не допустити викрадення комп'ютерної інформації. Наприклад, створення системи паролів, що у свою чергу не дозволить зловмисникові безперешкодно знайомитися з

конфіденційною комп'ютерною інформацією, що зберігатися у вашому комп'ютері, а тим більше викрасти її.

Насамкінець зазначимо, що в цій статті ми спробували об'єднати технічні вимоги стосовно безпечної експлуатації АЕОМ з правовими нормами, які мають за мету захищати ці правовідносини, та на основі цього визначити правила експлуатації автоматизованих електронно – обчислювальних машин. Аналіз чинного законодавства стосовно захисту комп'ютерної інформації свідчить, що воно потребує подальшого удосконалення, а також розробки принципово нових стандартів і правил безпечної експлуатації АЕОМ, де технічні норми були б тісно пов'язані з правом, які у своїй сукупності були б спрямовані протидіяти таким суспільно небезпечними наслідкам, як викрадення, перекручення або знищення комп'ютерної інформації в автоматизованих електронно – обчислювальних машинах.

Список літератури: 1. Науково-практичний коментар КК України від 5 квітня 2001 г./ Під ред. Мельника М.І., Хавронюка М.І . К., 2001. 2. Васильева В. С. Обслуживание ПК своими руками. Экспресс-курс. СПб., 2003. 3. Айков Д., Сейгер К., Фонсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями: Пер. с англ. М., 1999. 4. Расследование неправомерного доступа к компьютерной информации /Под ред. Н. Г. Шурухнова. М., 1999.

Надійшла до редколегії 16.03.04

І.В. Власенко, В.В.Федоров, М.О. Чміль

ВПЛИВ НОСІННЯ ЗАСОБІВ БРОНЕЗАХИСТУ НА ЕФЕКТИВНІСТЬ СТРІЛЬБИ З ВОГНЕПАЛЬНОЇ ЗБРОЇ

Поява засобів індивідуального бронезахисту в міліції обумовлена наявністю досить великої кількості вогнепальної і холодної зброї в арсеналі злочинного світу. Зброя часто застосовується проти працівників правопорядку, які одержують поранення і гинуть при виконанні своїх обов'язків. Наприклад, за роки незалежності України загинуло вже більш ніж 820 міліціонерів. Засоби бронезахисту, спеціально призначені для працівників правоохоронних органів, з'явилися на початку 70-х рр. Відлік ери бронезахисту для працівників міліції почався з прийняттям на озброєння бронежилета ЖЗТ–71.

З появою надійних засобів індивідуального захисту з'явилися певні труднощі в ефективному застосуванні бойової зброї і виконанні прийомів рукопашного бою. Дискомфорт, що відчувається бійцем при тривалому носінні бронежилета (БЖ), негативно позначається на функціональній діяльності організму в цілому, фіксуються функціональні і психічні порушення убік зниження його працездатності.

Носіння бронежилета погіршує функціональні особливості кожної людини. На думку 30% опитаних працівників міліції, БЖ заважає виконувати нахили, 24% – вільно плазувати, 25% – присідати, 3% – піднімати руки, 6% – бігти, 12% – користуватися зброєю.

Для підрозділів органів внутрішніх справ (ОВС) виникає проблема навчання умілому володінню бойовою зброєю при використанні засобів індивідуального захисту. Її рішення вимагає ретельного аналізу протиріч між