ГЛАВА ПЕТА. ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

В тази глава се изследват различни ефекти на информационните технологии при борбата със злоупотребите и корупцията. Авторът разглежда и въпроса за юридическата рамка, наложила се в последното десетилетие, в опит да се приведе законът в съответствие с технологиите, въпреки че тази рамка се простира далеч извън границите на по-тясната област на криминалните аспекти на корупцията. В подкрепа на ключовите законодателни аспекти е използвано и приложение.

Проявите на корупция, свързани с информационните технологии, имат отношение към повечето ситуации, разгледани в предишните глави. Тази част цели да насочи вниманието към специфичните мерки за борба с корупцията, свързани с информационните технологии, както и да разгледа традиционните мерки при работа с компютри.

5.1. ЗАЩО КОМПЮТРИТЕ ИЗИСКВАТ СПЕЦИАЛНО ВНИМАНИЕ?

Повечето важни системи, особено в публичния сектор, са компютризирани. Общият системен одиторски подход, определящ основните мерки за намаляване проявите на корупция или разкриването на такава, може да се прилага с еднаква сила и при компютризирани системи.

Понякога компютрите могат да прикриват действия по-успешно от писмените документи. Тяхната защита срещу неразрешен достъп и защитата на отчетността лесно може да бъде преодоляна. За повечето организации е трудно да се придържат към бързо променящите се технологии, което разширява полето за действие на престъпниците. Такива промени могат да поставят корумпираните служители в по-малко отговорна позиция.

Много злоупотреби, като неразрешен трансфер на парични суми, могат да бъдат извършени по-бързо благодарение на компютрите.

Компютърните злоупотреби се извършват предимно от доверени служители, за които техните ръководители или колеги не са допускали, че биха използвали информационните технологии по такъв начин. От една страна, компютърните технологии са все още новост, а, от друга, те се променят постоянно. Всяка крачка в развитието им носи допълнителни рискове или изисква нови защитни мерки. Целите и мотивите на извършителите остават същите.

Някои доказателства сочат човешкото его или предизвикателството като допълнителни мотиви за компютърните престъпления.

Проучване от 1990 г. показва, че компютърните злоупотреби са най-големи сред дейностите на доставчиците и кредиторите. Досега злоупотребите, свързани с въвеждането на данни, са най-сериозни. Една наскоро появила се форма на компютърна злоупотреба, компютърният вирус, е причинител на една трета от общия брой инциденти, отбелязани в изследването.

По-голямата част от компютърните злоупотреби според дефиницията на Европейската комисия са свързани с вътрешния персонал. Около една трета от всички инциденти са извършени от служители от ръководството или надзора, подчертаващо необходимостта от подробно преразглеждане и усилия от страна на управителното тяло при назначаването и контрола на персонала.

Останалата част от тази глава не предлага доказана методология за предотвратяване на конкретни престъпления в конкретни случаи, но насочвайки вниманието към някои специални характеристики, тя подчертава особеното значение на изпитани превантивни мерки и цели ограничаване на случаите на преднамерена компютърна злоупотреба.

5.2. РАЗДЕЛЕНИЕ НА ЗАДЪЛЖЕНИЯТА

Този тип контрол се среща във всички компютризирани системи, които извършват финансови операции или движение на активи. В общи линии разделението на задълженията е следното:

потребител - въвеждане на данните от потребителя на персонален компютър;

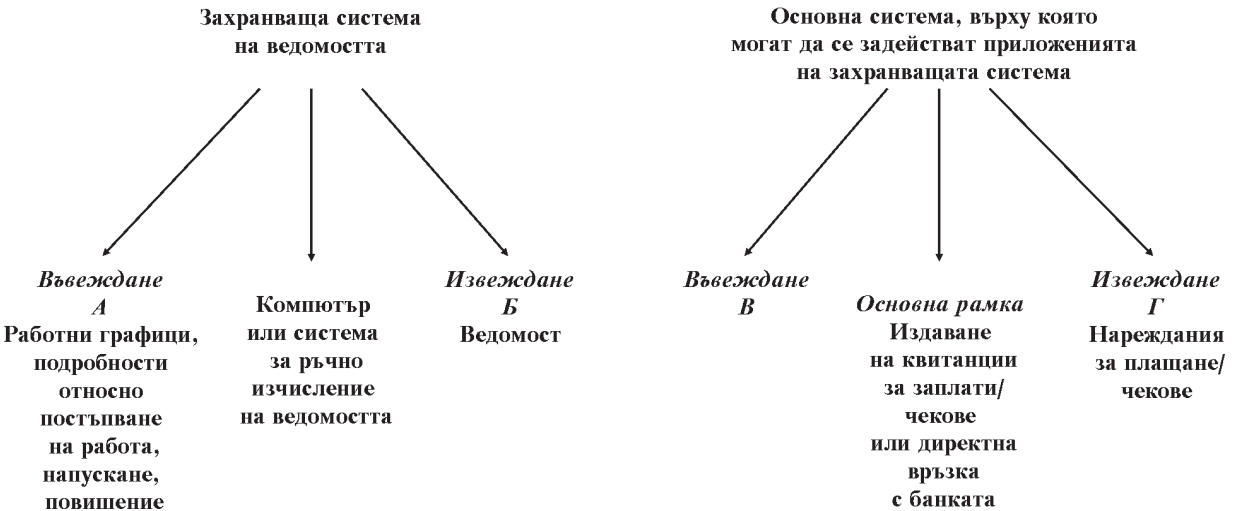
програмист - защита и поддръжка на операционните системи, софтуер и хардуер; развитие и корекция на програми;

оператор - обработка и охрана на ценни документи като чекове или лицензи;

оператор - актуализация и защита на данните.

Разделението на задълженията е сериозен проблем за голям брой сравнително малки обекти, или т. нар. отворени системи, които включват компютърни мрежи от свързани процесори или терминали, свързани с вторична процесорна единица. Наблюдението, стриктният контрол на паролите и ясният разбираем одиторски контрол могат да компенсират рисковете, до които води липсата на разделение в повечето случаи. Тази липса обаче може да увеличи рисковете от тайни споразумения, които са един от най-трудно разкриваемите методи на измама.

Фигура 3


Захранваща система
на ведомостта
Основна система, върху която
могат да се задействат приложенията
на захранващата система
Въвеждане
А
Работни графици,
подробности
относно
постъпване
на работа,
напускане,
повишение
Компютър
или система
за ръчно
изчисление
на ведомостта
Извеждане
Б
Ведомост
Въвеждане
В
Основна рамка
Издаване
на квитанции
за заплати/
чекове
или директна
връзка
с банката
Извеждане
Г
Нареждания
за плащане/
чекове

5.3. ПОСЛЕДВАЩИ ДЕЙСТВИЯ, СВЪРЗАНИ С КОМПЮТЪРНАТА ОБРАБОТКА

Те включват проверката на действителните плащания, трансфера на активи и т.н., обработвани на компютъра, и съпоставянето им с първоначалната документация, която удостоверява причините и пълномощията за извършване на сделката.

Компютърно изведените данни могат да бъдат потвърдени изцяло или лесно равнени при съпоставката им с ръчно обработените резултати или с други извеждания от захранващата система, която осигурява въвежданите данни на компютъра. Например със системата на ведомостта за заплати, виж фигура 3.

Компютър с основна рамка като тази на фигура 3 обикновено се използва за най-различни цели, всяка със своя собствена захранваща система. Например служителят, отговарящ за контрола по ведомостта, или счетоводителят на по-горното ниво трябва да е сигурен, че неговите инструкции са изпълнени веднага щом са получени. Проверката, независимо дали цялостна или частична, трябва да се направи поверително, но открито. Персоналът, включително всички потенциални извършители на злоупотреби, трябва да знаят за извършването на редовни и внезапни проверки и че цялата лична информация се пази като поверителна.

Същите цялостни съпоставяния между системите трябва да бъдат извършени за всички други основни раздели, като длъжници, кредитори и др.

5.4. ВЪВЕЖДАНЕ НА ДАННИ

Въпреки че компютризираните системи се използват за обработка на данни, тази обработка е възникнала от първоначалното въвеждане на писмена информация или необработени данни. Първоначално въвежданите данни могат да бъдат предоставени от външно лице, чрез документи, изготвени на компютър. При първоначалното въвеждане не съществува все още директна връзка между компютърните системи. Този етап е един от най-податливите на манипулации, свързани със злоупотреби. Тези рискове изискват превантивни мерки, които обхващат разрешение за достъп до данни и първоначален преглед на необработените данни.

Разрешение за въвеждане на данни

Разрешението трябва да е получено от потребителя, като се посочва определено ниво на отговорност. В идеалния случай сумите, въвеждани чрез

компютризирани захранващи системи, трябва директно да се проверяват и съпоставят с извежданите суми, които произвежда вече актуализираната система.

5.5. ПЪРВОНАЧАЛНА ПРОВЕРКА

Данните трябва да бъдат подложени на тест за валидност веднага след въвеждането. Те могат да включват проверка на минималните и максималните парични стойности за отделни сделки; сравнение на въвежданите записи със списъци на неприемливи параметри като например неприемливи дати за сделки, променени адреси и др. Най-общо казано, независимо от процедурите за програмирано преглеждане на данните, колкото по-рано се предприеме такова, толкова по-малък ще бъде рискът от извършване на злоупотреби.

5.6. АКТУАЛИЗАЦИЯ И ОБРАБОТКА НА ДАННИТЕ

Въвежданите данни обикновено се използват за актуализиране на постоянната информация за доставчици, длъжници, сметки за наем и др. Решаващо значение има строгата охрана на достъпа до тези постоянни данни, или т.нар. оперативни файлове. Ако подробности относно недвижима собственост, наеми, такси, и др. бъдат унищожени или по друг начин манипулирани, размерите на злоупотребата могат да останат напълно незабелязани за неограничен период от време. За да се нанесе сравнително тежка вреда при въвеждането на данните по една сделка, неразрешената намеса трябва да се повтори неколкократно, като всеки път се поема рискът от разкриване.

В идеалния случай потребителят на данните трябва да контролира или да извършва редовна проверка на оперативния файл, съхраняващ постоянна информация. Това се оказва трудно, особено в случаи, при които потребителят е малък отдел, който не може да отделя време за проверки. Но при всички случаи оперативният файл и контролните мерки, отнасящи се до поправките до този момент, трябва да бъдат редовно преглеждани от главен програмист, аналитик или компютърен одитор, който не е участвал в съставянето на операционната система или приложението на оперативния файл.

По време на актуализиране на главната оперативна система се изисква стандартното разделение на задълженията между оперативния персонал (включително служителите, извършващи подготовка на данните, въвеждане и контрол) и програмистите. Това разделение често не се изпълнява ежедневно, когато с програмистите се консултират относно неизправности в софтуера, кой-

то те са инсталирали или оформяли. На практика, като се има предвид тенденцията при много организации за преминаване към процесорни системи, този контрол често се оказва трудно приложим. Въпреки това, когато не се спази принципа на разделението, потенциалният риск от злоупотреби и корупция се увеличава, както показва и статистиката. Ръководството трябва да намери други мерки за контрол, компенсиращи липсата на разделение на задълженията.

Сред другите възможни начини за упражняване на контрол е редовният преглед на контролната информация на ръководството, отнасяща се до:

1) поправка на програми;

2) поправка на данни;

3) достъп (или неуспешни опити за достъп) до данните, особено по време на актуализация.

Други възможни контролни мерки, компенсиращи неадекватното разделение на задълженията, са допълнителният надзор и кодирането с пароли на важни данни, подлежащи на прехвърляне или актуализация.

5.7. ЮРИДИЧЕСКА СТРУКТУРА

В глава първа, читателят се запозна с това, как законът дефинира явлението „корупция“. По-долу са изложени два закона, опитващи се да разширят и осъвременят това понятие:

Закон за компютърните злоупотреби, 1990 г.

В продължение на много години, беше считано, че гражданското и криминалното право са били подходящите правни области за разрешаване на проблемите, свързани с компютърни престъпления. Най-съществено различие беше злодеянието, а не средството за неговото извършване. Явленията компютърно пиратство и компютърни вируси, изглежда, са главните постижения, които успяха да поставят под съмнение тази гледна точка. Пиратството се отнася към придобиването на неразрешен достъп до компютърни данни, най-често в резултат на липса на съответния контрол върху телефонните връзки или необезопасена мрежа.

Компютърният вирус е програмирана пречка за работа с данните, съхранени в паметта. Обикновено вирусът пристига посредством заразено или фалшифицирано програмно осигуряване, което е било закупено или копирано на магнитния диск. Също както един биологичен вирус той се възпроизвежда в процеса на изпълняване на програмите в компютъра. Най-обезпокояващата

характеристика на компютърния вирус е относителната лекота на трансмисия между организации и местоположения.

Оказва се, че нито едно от тези две съществени явления не са разгледани от закона по подобаващ начин. Всъщност твърди се, че има други подобни пропуски, като например липсата на мерки за борба с международните компютърни злоупотреби и също липсата на прецизна дефиниция за „компютър".

Закон за защита на данните, 1984 г.

Това е един любопитен и полезен закон, представляващ списък от законови предписания. Първоначално законът не е имал за цел да се занимава с корупцията. Той по-скоро цели да осигури акуратно и безопасно съхраняване на данни.

Законът също така се основава на осем принципа, направляващи събирането, съхраняването, употребата и разпространението на компютърно съхранявани данни. Тяхното най-важно качество е, че осигуряват безопасно съхраняване на данни, използвани единствено и само за законови и регистрирани цели.

Тази глава разглежда корупцията, свързана с информационните технологии. Компютризираната работна среда се е превърнала в характерна черта за почти всички органи на публичния сектор. Определени стандартни процедури, засягащи информационните технологии, придобиват допълнителна значимост. Важни са самостоятелната финансова ревизия и независимият подход при управлението на информационни технологии.

Това е така за случаите, в които се внедряват нови системи. Трябва да съществуват регулатори, отговарящи на следните цели:

1. Новата технология задоволява действителни нужди и е в съответствие с политиката и корпоративната стратегия на компанията.

2. Технологията се използва почтено, икономично и ефективно.

3. Прецизност на финансовата информация от всяка една система.

4. Адекватност на всяка система като цяло, и всички нейни форми на контрол.

Ако се вземе предвид необходимостта от придържане към технологичното развитие, то достигането до такъв начин на мислене би могло да представи на ръководителя или одитора оригинално професионално предизвикателство.