О.О. Арсірій, Т.Л. Будорацька, М.Г. Глава, Н.М. Журавльова, О.А. Журан, Л.М. Лінгур, Є.В. Малахов, В.П. Слободянюк, Т.П. Труфанова, Т.В. Філатова, А.А. Чугунов. Моделі, методи і засоби управління соціально-економічними об'єктами: монографія / О.О. Арсірій, Т.Л. Будорацька, М.Г. Глава, Н.М. Журавльова, О.А. Журан, Л.М. Лінгур, Є.В. Малахов, В.П. Слободянюк, Т.П. Труфанова, Т.В. Філатова, А.А. Чугунов**.** – Одеса: ОНПУ, 2016. – 225 с.

Л.М. Лінгур

2.2 Аналіз програмних продуктів інформаційної безпеки бізнесу

У сучасних умовах бізнес і підприємництво, державний апарат неможливо уявити без впровадження і використання інформаційних технологій. Новітні інформаційні технології, ERP - системи дають можливості комплексної автоматизації процесів збору, зберігання, обробки та використання інформації. Державні та комерційні структури широко використовують всі переваги комплексної автоматизації управлінської діяльності. [6]

Сучасне ведення бізнесу передбачає зростаючі обсяги інформації, прискорення динаміки бізнес-процесів для досягнення поставлених цілей. Оптимізація бізнесу, як завдання менеджменту підприємства, багато в чому базується на використанні новітніх IT - технологій, сучасних систем управління підприємством.

Діяльність будь-якого підприємства багато в чому пов'язана з проблемами інформаційної безпеки. Конфіденційність бізнес - інформації, інформаційні ресурси підприємства постійно знаходяться під загрозою, як зовнішньої, так і внутрішньої. І якщо питання зовнішньої безпеки з успіхом вирішуються апаратними та програмними засобами, то проблеми внутрішньої інформаційної безпеки часто залишаються без уваги. Рішення завдань внутрішньої інформаційної безпеки тим важливіше, чим більший доступ до інформаційних ресурсів компанії надається співробітникам для виконання виробничих завдань.

Безпека конфіденційної інформації підприємства, що ведуться і підготовлених бізнес-процесів, фінансової інформації може бути забезпечена

тільки в умовах дотримання політики безпеки. Інформаційна безпека діяльності підприємства є однією зі складових економічну безпеку виробничої системи.

На сьогоднішній момент в Україні практично не проводяться дослідження про фінансові втрати і втрати робочого часу через неконтрольоване доступу до мережі Інтернет. Більшість різних досліджень проводяться рекрутинговими та аудиторсько - консалтинговими компаніями (ФБК, Ipsos) [15]. Проведені ними дослідження показали, що близько 70% Інтернет - трафіку витрачається не в інтересах компаній, щорічно кожен співробітник проводить близько 50 годин робочого часу на сайтах і в програмах, що не мають відношення до роботи.

Певний інтерес представляє дисертаційна робота А.В. Бочкіна «Система моніторингу робочого часу в масштабі підприємства». У роботі розглядаються існуючі методики: моніторингу робочого часу співробітників; методики управління підприємством (ERP, CRM, BI); методики управління проектами; методики оцінки праці персоналу; методики обліку робочого часу. [7]

Важливим висновком роботи є необхідність проведення комплексного моніторингу робочого часу співробітників, задіяних на підприємстві з урахуванням як метрик питомих витрат часу, так і функціоналу використовуваних інформаційних систем, периферійних пристроїв, ресурсів мережі.

При цьому автор не розглядає існуючі програмні засоби моніторингу дій користувачів з позицій: наявного функціоналу, доступності готових рішень для бізнесу, простоти установки на мережу робочих станцій підприємства.

Мета дослідження - розглянути основні причини здійснення контролю і обліку робочого часу співробітників підприємства; аналіз сучасних програмних засобів моніторингу дій користувачів і визначення оптимальних продуктів з позицій виконуваного функціоналу.

Розглянемо причини моніторингу діяльності офісних працівників. Згідно з результатами масштабних досліджень, проведених низкою західних компаній,

головна причина низької ефективності праці і фінансових втрат організацій полягає у використанні співробітниками робочого часу не за призначенням. [7]

У проведенні досліджень були задіяні компанія IDC Research, Британський інститут громадської думки, газета Business Week, Американська асоціація менеджменту (American Management Association) і ряд великих інтернет-проектів, таких, як Vault.com, ZDNet Interactive, Websense та ін. [7]

За результатами проведених досліджень було названо багато причин для контролю та обліку робочого часу співробітників, а також ведення моніторингу дій користувачів і визначення на службових комп'ютерах програмного забезпечення, не передбаченого посадовими обов'язками:

По-перше, це втрати ефективного робочого часу. Яка не передбачена посадовими обов'язками діяльність співробітників протягом робочого дня призводить до втрати 40% ефективності праці.

По-друге, важко вести візуальний контроль за працюючими в офісі співробітниками. Не представляється можливим ведення постійного спостереження за виконанням ними роботи. Співробітники, які весь робочий день за комп'ютером та впевнені у відсутності контролю можуть присвячувати безпосереднього виконання роботи незначну частину часу.

Особливу проблему представляє і бездіяльність співробітників. Вчені Британського інституту громадської думки виявили, що офісні працівники в середньому кожен день витрачають 75 хвилин свого робочого часу бездіючи. Тим часом навіть годину втраченого часу у кожного співробітника для досить великої організації позначається на ефективності праці та витратності бізнесу самим кардинальним чином. [7]

Окремо необхідно виділити захист службової інформації та комерційної таємниці. Основна загроза криється саме всередині організації. У більшості випадків промислового шпигунства (58%) і витоку інформації через проломи в системі безпеки (60%) - справа рук співробітників компаній. [8] Вводячи і здійснюючи моніторинг персоналу, керівництво підприємства знижує ризик витоку інформації в кілька разів.

Найважливішим є оцінка економічного збитку. Майже 90% опитаних компаній зізналися в істотні збитки, викликаних діяльністю співробітників: нераціонально використовуються оплачуваний робочий час, канали зв'язку та інші ресурси компанії. [7]

Виходячи з вище наведених причин, можна зробити висновок про необхідність введення способів контролю діяльності та організації праці співробітників. Одним з таких засобів і є системи моніторингу робочого часу.

Система обліку та контролю робочого часу, або моніторингу є хорошим засобом аналізу діяльності співробітників підприємства. Завдяки широкому функціоналу системи моніторингу забезпечують своєчасне виявлення проблем організації роботи співробітників, оцінку їх професійних якостей і рівень ефективності діяльності структурних підрозділів компанії.

В останні роки великі американські і європейські компанії переходять до здійснення постійного контролю за діяльністю своїх співробітників. На західному ринку випускається безліч програм моніторингу. Сучасна IT-індустрія також надає корпоративному керівнику вибір серед програмних продуктів цього типу.

Всі програмні продукти моніторингу можна умовно розділити на три основні групи: системи виявлення фізичних підключень пристроїв і додатків; системи нецільового використання ресурсів мережі; системи визначення місця розташування об'єкта, маршрутизації об'єкта.

Перша група націлена на пошук, виявлення та перешкоджання подключениям різних пристроїв і програмного забезпечення як безпосередньо до комп'ютера користувача, так і через віддалений доступ.

Друга група здійснює стеження за процесами роботи користувачів, підключенням до спеціалізованим програмам - соцмережам, програмам швидких повідомлень, відеозв'язку, небезпечних сайтів і т.д.

Третя група стоїть осібно - це програми служби безпеки в чистому вигляді. Вони призначені в першу чергу для фізичного спостереження за транспортом, користувачем на основі GPS - навігації.

Останнім часом розробники, грунтуючись на вимогах клієнтів, розширюють функціонал пропонованих систем моніторингу, стираючи межі між групами.

Заслуговують на увагу такі програми, як система обліку і контролю робочого часу персоналу LanAgent, багата можливостями програма Security Curator, а також програмні продукти Boss Everyware, StaffCop Standard, Maxapt QuickEye Enterprise, Spector Pro, а також програмні продукти LizmaMonitor, Activity Monitor, WorkExaminer та ін .

Санкціоновані моніторингові програмні продукти використовуються адміністратором безпеки обчислювальної системи для забезпечення її наблюдаемості - властивості обчислювальної системи, що дозволяє фіксувати діяльність користувачів і процесів; використання пасивних об'єктів; однозначно встановлювати ідентифікатори причетних до певних подій користувачів і процесів, з метою запобігання порушення політики безпеки і / або забезпечення відповідальності за певні дії. [9] Повнота реалізації цієї властивості в системах моніторингу, дозволяє в різного ступеня вести автоматизований контроль дотримання співробітниками підприємства правил роботи на комп'ютерах і політики конфіденційності.

З якою метою встановлюють і використовують програми моніторингу?

Фахівцеві, відповідальному за інформаційну безпеку підприємства, найчастіше це сисадмін, з їх допомогою може визначати, локалізувати і контролювати:

- Спроби несанкціонованого доступу до конфіденційної інформації з точним зазначенням часу і мережевого робочого місця, з якого така спроба здійснювалася;

- Факти несанкціонованого встановлення програмного забезпечення;

- Використання персональних комп'ютерів в неробочий час і виявляти мета такого використання;

- Випадки несанкціонованого використання модемів в локальній мережі шляхом аналізу фактів запуску несанкціоноване встановлених спеціалізованих додатків;

- Всі випадки набору на клавіатурі критичних слів і словосполучень, підготовки будь-яких критичних документів, передача яких третім особам призведе до матеріального збитку;

- Факти нецільового використання персональних комп'ютерів:

- Отримувати достовірну інформацію, на підставі якої розроблятиметься політика інформаційної безпеки підприємства;

- Доступ до серверів і персональним комп'ютерам;

- Контакти власних дітей при серфінгу в мережі Інтернет;

- Проводити інформаційний аудит;

- Дослідити і розслідувати комп'ютерні інциденти;

- Проводити наукові дослідження, пов'язані з визначенням точності, оперативності та адекватності реагування персоналу на зовнішні впливи;

- Визначити завантаження комп'ютерних робочих місць підприємства;

- Відновити критичну інформацію після збоїв комп'ютерних систем;

і т.д. [9]

Всі перераховані можливості системи моніторингу є тим бажаним, але не досяжним функціоналом, певним теорією систем інформаційної безпеки. Тим не менше, ряд програмних продуктів в достатній мірі реалізує ці вимоги.

Найбільш популярними серед керівників підприємств і системних адміністраторів є наступні програмні продукти.

Більшість заходів моніторингу можна проводити за допомогою одного програмного комплексу: LanAgent- був апробований при роботі з 300 робочими станціями [11]. Це говорить про достатню масштабованості системи моніторингу. Однак розробники не вказують термін тривалості апробації та результати такої роботи.

LanAgent це лінійка програмних продуктів від простого LanAgent Standart до максимально розширеного LanAgent Enterprise. Всі продукти, що входять в

лінійку виконують моніторинг підключень і відключень USB - портів і каналів, контролюють набір текстів, символьних і кнопкових поєднань, що копіюються в буфер обміну текстів. За допомогою цих функцій виявляються витоку важливої корпоративної інформації.

Засоби складання звітності дозволяють роздруковувати звіти, конвертувати їх у різні типи, що дозволяє складати статистику по роботі користувачів і використання її в службових цілях [11, 6].

На рисунку 2.2 представлений звіт по одному комп'ютеру, щодо включений / виключений, активний / не активний. Це один зі звітів, як за змістом, так і за типом уявлення.

Розробник програмного продукту російська компанія ТОВ «NetworkProfi». Ліцензія умовно - безкоштовна на 15 днів для 3 комп'ютерів, об'єднаних в локальну мережу. Вартість подальшого придбання залежить від версії продукту і коливається від 300 грн. за LanAgent Standart на 2- 10 машин до 400 грн. за LanAgent Enterprise на 300 і більше машин.

Рисунок 2.2 - Вікно звіту по статистиці в системі LanAgent

Security Curator - це система забезпечення інформаційної безпеки нового покоління, що об'єднує в собі можливість спостереження за діяльністю співробітників, контролю їхніх дій і блокування потенційно небезпечних шляхів витоку інформації.

Security Curator виконує практично всі види моніторингу та логування персональних комп'ютерів співробітників. А саме: контроль основних шляхів витоку конфіденційної інформації та ефективності роботи співробітників; можливість відключення або блокування запуску додатків, процесів, операцій з файлами, сайтів і спілкування в чатах; система повідомлень про порушення політики безпеки; генерація деталізованих статистичних звітів про використання комп'ютерів організації; зручна система пошуку і фільтрації даних за ключовими словами [9]. Розробник програмного продукту ТОВ «Атом Безпека», Росія. Вартість ліцензії від 500 грн на 1 комп'ютер до 400 грн за 300 робочих станцій. Ліцензія на 1 рік, підтримка умовно - безкоштовна.

Наступна програма - є практично шпигунським софтом. Може бути встановлена на будь-який комп'ютер через віддалений доступ і не виявляється через Диспетчер завдань. Системний адміністратор має права для її установки, а от спроби виявити роботу Boss EveryWare сполучені з певними труднощами. Для цього необхідна як мінімум програма Process Explorer від Microsoft.

Boss EveryWare - логует всі програми, що запускаються користувачем, і враховує час, витрачений на них. Програма зчитує всі надруковані користувачем символи, таким чином, логіни і паролі, набрана кореспонденція стають відомі сисадміну. Boss EveryWare реєструє час простою комп'ютера, повідомляє адміністратора мережі про встановлені програми, яке програмне забезпечення було використано і які веб - сайти були відвідані.

Boss EveryWare має як відкритий так і прихований режим роботи. Тобто може виводити користувачеві інформацію на заборонені до використання того чи іншого додатка, а може бути вести приховане спостереження, перериваючи роботу користувача в критичних випадках: наприклад при спробі відправки файлу невідомому адресатові. Дана програма захищена паролем і до неї має

доступ тільки мережевий адміністратор [10]. Ліцензія на програму умовно - безкоштовна, на 1 рік вартість близько 500 грн.

Наступний програмний продукт також представляє ТОВ «Атом Безпека», Росія. Вартість ліцензії від 378 грн на 1 комп'ютер до 207 грн за 300 робочих станцій. Ліцензія на 1 рік, підтримка умовно - безкоштовна.

Відмінність між продуктами одного розробника в першу чергу в акцентах: StaffCop Standard орієнтований на моніторинг дій користувачів в Мережі, а Security Curator - на виявлення додаткових пристроїв, введення - виведення інформації, тобто на фізичну витік інформації.

StaffCop Standard - система корпоративної інформаційної безпеки.

StaffCop Standard контролює всі дії співробітників за робочими комп'ютерами і дозволяє отримувати дані про роботу кожного з них як в режимі on-line, так і у вигляді наочних звітів за будь-який період часу. [9]

Програма дозволяє спостерігачеві моніторити соціальні мережі: ВКонтакте, Однокласники і Facebook, Amigo. Надає можливість переглядати всі пошукові запити працівників в Яндексі, Google, Рамблер і багатьох інших пошукових системах.

Директор, HR - менеджер або системний адміністратор отримує результати роботи програми в різному вигляді і формі: діаграми роботи з програмами та іграми, діаграми відвідування сайтів і спілкування в ICQ. Крім загального уявлення з моніторингу, передбачена можливість перегляду листування в ICQ, Mail.Ru агенту та інших програмах обміну повідомленнями. Логуються всі дії з файлами, історія надрукованих документів, підключені USB пристрої, встановлені програми та багато іншого. [9]

Розглянуті програмні продукти з успіхом застосовуються на підприємствах з великим обсягом інформаційних потоків, робочих станцій, розгалуженою мережею підрозділів. Вони можуть бути рекомендовані для впровадження в банківській справі, агентствах нерухомості, мережевих торгових підприємствах тощо

Перераховані програмні продукти мають ряд хороших можливостей, але розробники не вказують будь-яких недоліків. Тим не менш, недоліки існують.

По-перше, всі системи моніторингу припускають приховану від користувача установку і роботу. Програми запускаються з автозавантаження, що збільшує час запуску комп'ютера, кілька «гальмує» його роботу. Досвідчені користувачі, виявивши засоби стеження (наприклад, за допомогою Провідника Windows) можуть стерти їх. Також користувачі віддалених робочих станцій можуть використовувати Захисник Windows, блокуючи роботу підозрілих портів і процесів.

По-друге, якщо сисадміни відстежують з'єднання не так на кожному комп'ютері, що дуже складно при великій кількості робочих станцій, а на корпоративному проксі-сервері, то можливе використання програмних продуктів Jap An.On (анонімність в мережі).

По-третє, чим більше робочих станцій, комп'ютерів в корпоративній мережі, тим більше роботи з моніторингу, перевірці результатів систем контролю робочого часу. Обсяг інформації, яка збирається системою моніторингу і вимагає прийняття рішень з окремим співробітникам, росте в геометричній прогресії. Отже, необхідно розглядати питання про створення окремої служби на підприємстві, а це додаткові витрати.

А хто буде спостерігати за наглядачами ?!

Таким чином, можна зробити висновок про введення в політику фірми відкритого заборони на використання комп'ютерів і мережевих ресурсів не за призначенням, в особистих цілях. Але й системами моніторингу нехтувати не варто.

Наступна система являє собою одну з цілої лінійки програмних продуктів і має дещо інше застосування, це система фізичного виявлення об'єкта, фактично система стеження. Системи лінійки «ГЛОСАВ» з успіхом застосовуються в організаціях, що надають послуги доставки вантажів, у тому числі небезпечних, інкасації як банківської, так і об'єктної, спостереження за пасажиро-перевезеннями, розробка маршрутів охорони об'єктів і т.і.

Фактично система являє собою персональний моніторинг, будучи при цьому альтернативним засобом підвищення ефективності роботи персоналу. Система надає точну і достовірну інформацію про місцезнаходження транспортного засобу та / або співробітників. [12]

Така інформація використовується різними відділами підприємства для аналізу та розробки маршрутів доставки вантажів, складання та планування графіків виконуваних робіт, підвищення продуктивності співробітників і устаткування компанії, зниження витрат, підвищення рівня задоволеності клієнтів обслуговуванням.

Особливо важливим є планування маршрутів і захист цієї інформації для служби інкасації банків, охорони та доставки цінних вантажів, служби безпеки об'єктів.

Розробник систем ГЛОСАВ ТОВ «РОСТТЕХНОТОРГ - Глобальні системи автоматизації», м. Ростов - на - Дону, Росія. Вартість готових рішень залежить від кількості об'єктів, їх обладнання, можливості і необхідності переналагодження програмних рішень обумовлюється в кожному конкретному випадку.

Особливий інтерес представляє з позиції дружності до користувачам система Yaware.

На відміну від раніше розглянутих програмних продуктів, Yaware відкрита для користувача система, результати її роботи доступні як для керівника, так і для окремого співробітника.

З одного боку, керівник може бачити інформацію про діяльність всіх співробітників, з іншого - кожен користувач може проаналізувати свою роботу за певний період часу. Таким чином, крім засоби стеження, система є і засобом тайм-менеджменту.

Yaware - це інтернет-сервіс для контролю користувача активності на комп'ютері. Система автоматично збирає інформацію про те, чим займається співробітник на ПК, фіксуючи запуск додатків і Інтернет-сайтів (активну вкладку), час їх активності та неактивності, після чого вибудовує графіки

продуктивності роботи. Сервіс автоматично записує початок / закінчення робочого дня, перерви, фактично відпрацьований час. [13]

Програмний комплекс Yaware визначає які додатки використовувалися на комп'ютері в перебігу робочого дня, фіксується час включення і виключення комп'ютера. Якщо в роботі співробітників передбачена діяльність не пов'язана з активною роботою за комп'ютером, то така інформація може бути внесена заздалегідь і система виступає як планувальник, нагадуючи користувачеві про заплановані події (виїзд до клієнта, нарада, обідня перерва і т.д.)

Система формує наочні звіти у вигляді графіків і діаграм Ганта (Рисунок 2.3). Всі графіки та діаграми забезпечені спливаючими вікнами пояснень. Інформація доступна в режимі онлайн, в особистому кабінеті, з ноутбука або мобільного. Можливе отримання звітів на email, вказавши графік.[13].

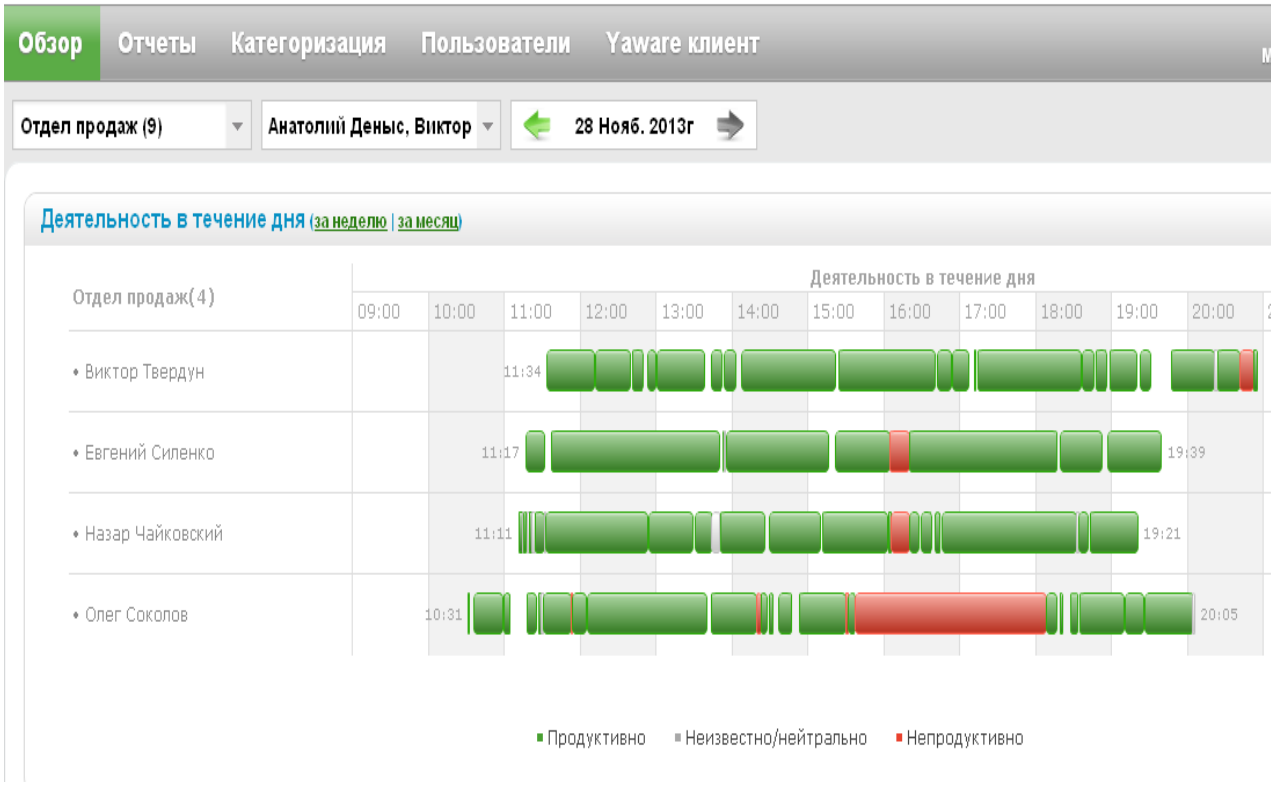

Рисунок 2.3- Діаграма Ганта по діяльності співробітників одного відділу

Використання системи Yaware для особистих цілей на домашньому комп'ютері, наприклад, безкоштовно. Представляє інтерес можливість установки системи в навчальних лабораторіях. Така установка вимагає деяких

додаткових налаштувань, але не є неможливою. Обмеження виникають через коротких тимчасових рамок (90 хвилин навчального часу) і кількості користувачів на одній робочій станції. Інформація отримана від розробників в особистому спілкуванні.

Розробник компанія Yaware, Тернопіль, Україна. Вартість ліцензії від 480 грн. на 1 комп'ютер до 420 від 200 робочих місць. Для особистого користування на 1 машину установка безкоштовно, але функціонал суттєво урізаний.

У таблиці 2.7 наведено порівняльний аналіз можливостей низки поширених програм моніторингу [6]. Провівши порівняльний аналіз найбільш поширених програмних продуктів моніторингу, можна відзначити, що жоден з них не підтримує повністю запитуваний функціонал. З позицій інформаційної безпеки для компаній, що не використовують у своїй діяльності мережу Інтернет, кращим вибором будуть продукти LanAgent або Security Curator. І, навпаки: для тих організацій, чиї товари та послуги просуваються по принципам електронної комерції, будуть корисні Boss EveryWare і Staff Cop Standart. Тим не менш, у розробників залишається ще досить неохоплених пунктів поліпшення функціоналу програмних продуктів.

Таблиця 2.7 - Порівняльний аналіз функціоналу систем моніторингу

№	Функціонал	Lan Agent	Security Curator	Yaware	Boss EveryWare	Staff Cop Standart	ГЛОСАВ
1	Моніторинг запам'ятовуючих пристроїв	+				+	
2	Блокування запуску різних додатків	+	+				
3	Контроль критичного набору, буфера обміну	+			+	+	
4	Експорт звітів в популярні формати даних	+	+	+	+	+	+
5	Розмежування прав доступу до Інформації, що збирається	+	+		+	+	+

6	Визначення графікаробочого часу		+	+	+	+	+
7	Моніторинг соц. сетей			+	+	+	+

Більш простим методом уберегти кампанію від втрат, а співробітників від осуду - відключити повністю доступ до мережі Інтернет. Але такий метод не можливий в тих організаціях, чия діяльність, так чи інакше пов'язана з мережею. У цьому випадку використання спеціальних програм моніторингу допоможе підприємцям скоротити втрати робочого часу, а в деяких випадках і інформації. Однак слід пам'ятати, що установка таких програм на комп'ютери співробітників повинна бути регламентована трудовим договором. В іншому випадку, це може бути розцінене, як порушення прав людини і оскаржена в судовому порядку.

Як правило, у більшості комерційних компаній в умовах трудового договору регламентовано використання ресурсів мережі Інтернет на робочому місці, або ж існує інструкція, яка доводиться до відома співробітників при прийомі на роботу.

Аналіз досліджень проведених різними представницькими організаціями за представленою проблемі в 2009 - 10 і 2011 - 12 роках показує, що, незважаючи на всі застосовувані засоби і методи, поліпшення систем моніторингу, посилення засобів захисту корпоративної таємниці, не дає будь - яких відчутних результатів. Зменшуються фізичні витоку інформації, збільшується нецільове використання робочого часу, ресурсів мережі і т.д. Напрошується висновок, що зміни повинні торкнутися не тільки діяльності співробітників, але дій менеджменту підприємств.

Отже, на протязі дослідження розглянуто причини введення програм моніторингу діяльності працівників, запропоновані різні за можливостями і цілям засоби моніторингу. Визначено програмні продукти оптимальні для використання в залежності від виду діяльності підприємства та надано рекомендації щодо їх використання.

Література

6. L. Lingur The information security software in business / Iesina O., Lingur L. // Економіка: реалії часу. Науковий журнал. Одеса, 2013. – №5. – С.175-180

7. Бочкин А.В. Система мониторинга рабочего времени в масштабе предприятия: автореф. дис. на соискание степени док. тех. наук: спец. 05.13.10 спец.: «Управление в социальных и экономических системах» / Бочкин Александр Викторович; Пенз. гос. ун-т - Саранск, 2009 - Количество страниц: 147 с. ил. Саранск, 2009 147 с. [Электронный ресурс]: — Режим доступа к журн.: http://www.lib.ua-ru.net/diss/cont/357519.html, 21.11.2013

8. 5 причин мониторинга деятельности офисных работников. [Электронный ресурс]: — Режим доступа к журн.: http://www.avangard-sb.ru/securitysystem/worktime.php, 10.04.2013

9. Н.Д. Красноступ, Д.В. Кудин. Шпионские программы и новейшие методы защиты от них. [Электронный ресурс]: — Режим доступа к журн.: http://bozza.ru/art-75.html, 12.04.2013

10. А.Жмерик. Boss – EveryWare Описание программного продукта [Электронный ресурс]: — Режим доступа к журн.: http://www.softsoft.ru/security-privacy/covert-surveillance/7922.htm, 8.04. 2013

11. Описание программного продукта LanAgent. [Электронный ресурс]: - Режим доступа к журн: http://www.lanagent.ru/lanagent_func.html, 20.04. 2013

12. Система мониторинга персонала ГЛОСАВ. [Электронный ресурс]: — Режим доступа к журн.: http://rttg.ru/index.php/services/monitoring/11-informationcat, 6.05.2013

13. Начинаем бой с рабочей ленью. Обзор сервиса Yaware. [Электронный ресурс]: — Режим доступа к журн.:

http://internetno.net/category/obzoryi/nachinaem_boj_s_rabochej_lenyu_obzor_servisa_yaware/, 22.11.2013

14. Соцсети на рабочем месте – зло или благо? [Электронный ресурс]: — Режим доступа к журн.: http://www.odmu.od.ua/statti/socseti-na-rabochem-meste-zlo-ili-blago/, 15.05.2013

15. В плену социальных сетей. [Электронный ресурс]: — Режим доступа к журн.: http://kiev.rabota.ru/rabotodateljam/upravlenie_personalom/v_plenu_sotsialnyh_setej.html, 20.11.2013

16. Соцсети на работе: пожиратель времени или полезный инструмент: [Электронный ресурс]: — Режим доступа к журн.: http://ubr.ua/labor-market/life-at-work/socseti-na-rabote-pojiratel-vremeni-ili-poleznyi-instrument-249379, 21.11.2013