Литература: ***1.*** *Бортников А. Н., Губин С. В., Комаров И. В., Майоров В. И. Результаты экспериментальной оценки эффективности защиты речевой информации от утечки по техническим каналам при использовании различных видов помех.// Информация и безопасность. – Воронеж, 1999. – Выпуск № 4.* ***2.*** *НД ТЗІ – Р – 001 – 2000. Засоби активного захисту мовної інформації з акустичними та віброакустичними джерелами випромінювання. Класифікація та загальні технічні вимоги. НД ТЗІ – Р – 001 – 2000. ДСТСЗІ СБ України. – Київ.: - 2000. – 9 с.* ***3.*** *Архипов А. Е., Журавлев В. Н., Завьялов С. Н. Корреляционный анализ сигналов аддитивного маскирования речи. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2006. – № 12. – С. 11 – 18.* ***4.*** *Покровский Н. Б. Расчет и измерение разборчивости речи. - М.: Связьиздат, 1962. – 392 с.* ***5.*** *Михайлов В. Г., Златоустов Л. В. Измерение параметров речи/ Под ред. М. А. Сапожкова. – М.: Радио и связь, 1987. – 168 с.*

УДК 681.3.07

ПРАВОВЫЕ И ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ ПРИМЕНЕНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ КОНТРОЛЯ ПЕРСОНАЛА ПРИ РЕАЛИЗАЦИИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Валерий Слепцов, Владимир Журавлев
Запорожский национальный технический университет

Анотація: **Розглянуто питання правового обгрунтування застосування технічних засобів контролю персоналу на підприємствах України, впливу цього чинника на лояльність співробітників.**
Summary: **The questions of legal substantiation of the application of staff supervision technical facilities on the Ukraine enterprises and the influence of this factor for the staff loyalty are under review.**
Ключевые слова: **Конфиденциальная информация, технические средства контроля, лояльность сотрудников, психологический дискомфорт, законодательство Украины.**

I Введение. Постановка задачи

Уязвимость любой информационной системы определяется совокупностью техногенных угроз и угроз, исходящих от персонала, который обслуживает эту систему и пользуется ее услугами [1]. Решение проблем, связанных с человеческим фактором, основано на организационно-управленческих мерах, часть из которых реализуется с применением специализированных аппаратно-программных средств [2]. В наибольшей степени такое техническое обеспечение присуще контрольным мероприятиям, в процессе которых осуществляется мониторинг информационных сообщений сотрудников.

Руководители частных компаний высокоразвитых стран все чаще прибегают к слежке за своим персоналом. По данным Ассоциации американских менеджеров, в 2004 году в 73,5% частных организаций США был установлен периодический или постоянный контроль над действиями служащих, тогда как в 1997 г. это практиковалось только в 35 % фирм [3]. Данные по Украине, к сожалению, отсутствуют, но, думается, что вполне правомерно предположение об активизации применения технических средств контроля (ТСК) персонала в деятельности организаций с целью обеспечения информационной безопасности (ИБ) и в нашей стране.

Реализация политики мониторинга сотрудников в процессе их служебной деятельности чаще всего осуществляется с использованием средств видеонаблюдения, контроля телефонных переговоров, средства просмотра электронной корреспонденции или наблюдения за работой в сети Интернет. Указанная тенденция объясняется следующими причинами:

- сохранность коммерческой тайны организации определяется, прежде всего, уровнем управления персоналом, составной частью которого является контроль над его деятельностью;
- ТСК стали доступны не только для крупных корпораций, но и для средних и малых предприятий;
- многих руководителей привлекает возможность негласного использования ТСК для получения конфиденциальной информации о своих подчиненных и соблюдении ими трудовой дисциплины;
- результаты мониторинга легко документируются с возможностью их использования как средства давления на сотрудников или как основание для привлечения их к ответственности в случае несоблюдения регламентных требований или трудовой дисциплины.

Как правило, руководители, принимающие решение об использовании ТСК, не в полной мере

представляют возможные негативные последствия таких действий, обусловленные необходимостью соблюдения прав работника и поддержания нужного психологического климата в трудовом коллективе. Проблема усугубляется отсутствием в украинском законодательстве норм, устанавливающих, хотя бы в общих чертах, требования к процессу мониторинга деятельности сотрудников. В публикациях по обеспечению информационной безопасности этому вопросу также не уделяется, по нашему мнению, достаточного внимания.

В настоящей работе сделана попытка правового обоснования использования ТСК и анализа возможных негативных последствий мониторинга персонала, с учетом как юридических, так и психологических аспектов этой деятельности.

II Основная часть

Применение ТСК в рамках проводимой политики безопасности в общем случае позволяет решить с той или иной полнотой следующие основные задачи:

- предупреждение и выявление случаев утечки конфиденциальной информации;
- осуществление контроля выполнения сотрудниками правил доступа к информационным ресурсам и на объекты информационной деятельности, определенные политикой безопасности;
- документирование фактов предательства интересов организации ее сотрудниками;
- предупреждение преступных действий со стороны криминалитета и нарушителей ИБ со стороны внешней среды;
- оценка лояльности персонала, эффективности и производительности труда сотрудников;
- контроль соблюдения трудовой дисциплины.

Многофункциональность и эффективность ТСК является стимулирующим фактором к их более активному распространению и использованию. Однако правовые проблемы ограничения тайны связи или защиты персональных данных могут стать серьезным препятствием к этому. Анализ законодательной базы позволяет сделать вывод о практическом отсутствии юридической основы для такого рода деятельности менеджмента предприятий в Украине.

Прежде всего, необходимо иметь в виду, что в результате применения ТСК могут быть нарушены предусмотренные ст. 31 Конституции Украины личные права работников: "Каждому гарантируется тайна переписки, телефонных переговоров, телеграфной и другой корреспонденции. Исключения могут быть установлены только судом в случаях, предусмотренных законом, с целью предотвратить преступление или выяснить истину во время расследования уголовного дела, если иными способами получить информацию невозможно". Согласно ст. 32 "... не допускается сбор, хранение, использование и распространение конфиденциальной информации о лице ***без его согласия***, кроме случаев, определенных законом, и только в интересах национальной безопасности, экономического благосостояния и прав человека". В первой из приведенных норме основного закона не уточняется характер переписки или телефонных переговоров, следовательно, нет оснований для ограничения ее действия по любым другим причинам, кроме указанных в Конституции. Использование службами безопасности негосударственных структур средств контроля телефонных переговоров и электронной почты сотрудников в указанных выше целях, разумеется, не подпадает под исключения, предусмотренные ст. 31. Законодательство Украины никаких особых прав руководителям и предпринимателям в плане вмешательства в переписку и переговоры сотрудников не дает, возможности ограничения ими тайны связи не предусматривает. Следовательно, лица, занимающиеся такого рода деятельностью, могут быть привлечены к уголовной ответственности по ст. 182 УК Украины ("Нарушение неприкосновенности личной жизни"), ст. 163 ("Нарушение тайны переписки, телефонных переговоров, телеграфной или иной корреспонденции, передаваемой средствами связи или через компьютер"). Кроме того, поскольку ТСК в некоторых случаях могут быть отнесены к специальным техническим средствам, к правонарушителям может быть применена и ст. 359 УК, устанавливающая уголовную ответственность за незаконное использование специальных технических средств негласного получения информации.

На защиту интересов личности направлена и норма ст. 10 Закона Украины "О предпринимательстве", в соответствии с которой предприниматель обязан "... не нарушать прав и интересов граждан, ... которые охраняются законом".

Поскольку в ходе использования ТСК может быть получена конфиденциальная информация о сотрудниках, вступает в действие ст. 32 Конституции, запрещающей такую деятельность ***без согласия лица,*** в отношении которого проводится мониторинг. Указанная норма не предусматривает исключений, законодательством не установлена возможность сбора, хранения, использования и распространения персональных данных работодателем, если он не принадлежит к государственным структурам, обладающими специальными полномочиями.

Однако такой подход применительно не к частным лицам, а сотрудникам тех или иных организаций не учитывает особенности трудовых взаимоотношений работника и нанимателя. На наш взгляд, вполне обоснованно замечает Емельянников М. [4], что "... служебный телефон, компьютер с доступом к электронной почте и сети Интернет являются рабочими инструментами, предоставленными работодателем своему сотруднику для выполнения служебных обязанностей, а вовсе не для использования в личных целях". Абонентами телефонной сети и электронной почты является организация – юридическое лицо, или ее структурное подразделение, а не конкретный сотрудник. Поэтому работодатель, несущий финансовую ответственность за действия своих сотрудников, в соответствии со статьями 13, 27 закона "О предприятиях в Украине" имеет право контроля использования этих инструментов. В противном случае он теряет одну из наиболее эффективных возможностей управления рисками. Этим же нормативным актом руководителю предприятия делегируется право определять порядок защиты сведений, составляющих коммерческую тайну (ст. 30). Важно также подчеркнуть, что сама природа трудового договора (ст. 21 Трудового кодекса Украины) не предусматривает обязанность работодателя обеспечить условия частной жизни, отдельной от функционирования предприятия, а потому предприятие вправе осуществлять контроль использования предоставленных сотрудникам ресурсов, не нарушая требований законодательства. Другое дело, что в некоторых случаях достаточно сложно определить критерий осуществления трудовой деятельности, особенно при работе в сети Интернет и при использовании электронной почты.

Проблемы, связанные с необходимостью соблюдения указанных выше правовых норм, наверняка возникнут в том случае, если в организации не определена политика безопасности, отсутствует нормативно-правовая база, регламентирующая использование средств коммуникации и доступа в Интернет. Прежде всего, необходимо открытое признание руководством факта мониторинга с четким обоснованием его причин. В трудовом договоре, опираясь на статью 21 Трудового кодекса Украины, можно предусмотреть ответственность сотрудников за не целевое использование телекоммуникационных средств, предоставленных предприятием в целях более эффективного выполнения работ. Во всех должностных инструкциях должно быть оговорено обязательство сотрудника соблюдать установленные правила пользования средствами связи. Первое и главное требование регламента – использование в рабочее время телефона, факса, электронной почты, доступа в Интернет только для выполнения служебных задач. Далее, всем служащим должно быть официально объявлено путем письменного уведомления о проведении администрацией мониторинга служебных переговоров и отправляемых сообщений (в соответствии с условиями коллективного трудового договора), как с вмешательством соответствующих должностных лиц, так и в автоматическом режиме, с использованием специальных аппаратно-программных средств. Обязательно необходимо указать и цель проведения такого мониторинга – предупреждение разглашения или передачи сведений, составляющих коммерческую тайну организации. При этом, необходимо иметь в виду, что меры контроля с использованием ТСК, заложенные в трудовой договор, могут быть расценены работником и контролирующими органами как ухудшающие состояние работника в сравнении с законодательством Украины о труде и, следовательно, при возникновении конфликтных ситуаций суды, основываясь на ст. 9 Трудового кодекса Украины, могут признать их неправомерными.

Указанная регламентация, конечно, не исключает случаев неумышленного доступа уполномоченных представителей администрации к конфиденциальной информации сотрудников, злоупотребляющих своими правами при использовании служебных средств коммуникаций. В этом случае важно разработать ***механизм, предупреждающий разглашение*** таких сведений, чтобы исключить возможность предъявления судебных исков со стороны отдельных персоналий на основании ст. 16 Гражданского кодекса Украины, предусматривающей судебную защиту гражданских прав и интересов личности. К данному виду деятельности желательно привлекать только специально обученных сотрудников, доверие к которым со стороны администрации должно быть абсолютным. Самое главное – это исключить возможность вторжения в частную жизнь, проникновение в личную тайну, получение и распространение так называемой "чувствительной" информации, которая защищается международным правом и законодательством Украины.

Другая проблема, которую нельзя не учитывать администрации, принимающей решение об использовании ТСК, – проблема мотивации сотрудников. Наряду с дисциплинирующим фактором, присущим любым мерам контроля, несомненно, имеет место различие в восприятии ограничений разными людьми. Для большинства – это специфическая форма психологического воздействия, нагнетающего в коллективе напряжение, что, в конечном счете, способствует возникновению межличностных конфликтов и эмоциональных срывов [5]. Последние могут возникнуть из-за чувства унижения личного достоинства и несправедливости от вторжения в личную жизнь. Говорить в такой обстановке о лояльности сотрудников к

администрации не приходится. Становятся вполне вероятными случаи противодействия контролю, доносы и прямого предательства. Налицо, таким образом, противоречие между целями, преследуемыми администрацией и трудно предсказуемыми последствиями тотального контроля, которые не только могут свести на нет эффект применения ТСК, но даже способствовать усугублению положения дел, связанных с защитой конфиденциальной информации. Смягчить негативные последствия контроля может правильная политика администрации. Если она ясно и четко формулирует причины, заставляющие проводить мониторинг и способы его осуществления, предусматривает разъяснение персоналу, что понимается под допустимым поведением в повседневной трудовой жизни, не допускает разглашения персональных данных, адаптация сотрудников к требованиям политики безопасности, предусматривающей использование ТСК, может пройти безболезненно.

Реализация новых подходов к проблеме обеспечения ИБ в процессе управления персоналом требует изучения, анализа и осмысления международных правовых документов и зарубежного опыта в этом вопросе. Международное признание важности проблемы персональных данных было закреплено в 1981 году принятием странами Совета Европы Конвенции по защите данных о личности при автоматизированной обработке информации. Конвенция исходит из того, что права и интересы личности в условиях применения новейших информационных технологий, компьютерных и телекоммуникационных средств могут быть нарушены в результате несанкционированного использования сведений о личности ей же во вред, тем самым, сведя на нет ее природные, жизненные права, являющиеся основой свободы, общей справедливости и мира. Указанные права следует защищать властью закона. На основе этого положения и требований других международных документов, определяющих основные принципы защиты частного интереса в области персональных данных, построены системы некоторых национальных законодательств.

Например, в США в ряде отраслей (здравоохранение, федеральные органы) установлены ограничения на порядок контроля персонала [6]. Соглашения с профсоюзами регламентируют порядок надзора за их членами. Кроме того, регулируются виды и способы физического мониторинга на рабочих местах. Существуют ограничения и на запись звука – запрещено записывать его при помощи физических систем наблюдения, а телефонные разговоры не могут записываться без согласия самого работника. Во многих штатах США для прослушивания телефонного разговора требуется согласие всех заинтересованных сторон.

В Европейском Союзе право на тайну частной жизни считается одной из фундаментальных свобод человека, и электронный мониторинг в значительной мере ограничен законодательными актами. В Великобритании в 2003 г. был принят Свод правил, дополняющих Акт о защите информации, расширительно трактующих право на защиту частной и семейной жизни, а также на защиту частной корреспонденции [7]. Новые нормы не запрещают контроль, они четко прописывают правила поведения участников трудовых отношений. В частности, работодатели должны доказывать, что контроль за служащими необходим для защиты интересов компании. При этом не допускается сбор информации, которая выходит за рамки внутри корпоративных отношений.

В подавляющем же большинстве стран мира использование ТСК коммерческими организациями находится де-факто в коллизии с рядом правовых норм. Например, в России, как и в Украине, законодательство не предусматривает возможность предприятия осуществлять мониторинг персонала с использованием технических средств наблюдения.

III Выводы

Контроль персонала с применением ТСК, направленный на обеспечение ИБ и решение других задач, связанных с повышением эффективности работы сотрудников, находит все большее количество сторонников в предпринимательской среде Украины. При достаточном юридическом обеспечении таких мер наниматель вправе рассчитывать на судебную поддержку. Однако не проработанность украинского законодательства, рассматривающего абонента связи лишь как частное лицо, не позволяет дать однозначный ответ на вопрос о правах работодателя и порядке организации и допустимых границах такого мониторинга. Необходимы правовые нормы, в которых бы четко прописывались процедура осуществления контроля, права работодателя и работника с точки зрения необходимости защиты интересов организации и личности. Уместно, на наш взгляд, изложить такие нормы в не принятом пока законе "О коммерческой тайне", необходимость принятия которого чрезвычайно актуальна. Не менее актуален и вопрос о законодательном регулировании общественных отношений, возникающих при сборе, обработке и распространении персональных данных.

Литература: ***1.*** *Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. - Москва * Санкт-Петербург * Киев: ООО "ТИД "ДС", 2002. - 688 с.* ***2.*** *Тетяна Тардаскіна.*

Організаційно-управлінські аспекти системи інформаційної безпеки. // "Правове, нормативне та метролргічне забезпечення систем і захисту інформації в Україні". Вип. 11, 2005. С. 28 – 33. ***3.*** *Гусев В. С. Экономика и организация безопасности хозяйствующих субъектов. СПб.: "Питер". 2004. - С. 268.* ***4.*** *Контроль собственных сотрудников - преступление или обязанность? Защита информации. Конфидент. 2003. - № 3.* ***5.*** *Слепцов В. И., Журавлев В. Н., Романюк И. Н. Влияние межличностных психологических отношений на эффективность политики информационной безопасности предприятия // "Бизнес и безопасность". Киев. № 2. - 2006. С. 154 – 156.* ***6.*** *Дейнтри Даффи. Как надо подглядывать. // CSO, № 2, 2003.* ***7.*** *М. Дашьян. E-spy Methods в процессе управления персоналом. // Управление персоналом. - М.: № 1 – 2, 2005, - с. 29 – 31.*

УДК 681.3

ОБОСНОВАНИЕ НАПРАВЛЕНИЙ МОДЕРНИЗАЦИИ ВЕДОМСТВЕННОЙ СИСТЕМЫ РАДИОСВЯЗИ С ПОДВИЖНЫМИ ОБЪЕКТАМИ ЗА СЧЁТ ПРИМЕНЕНИЯ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ

Борис Горлинский, Сергей Ливенцев, Сергей Зайцев
Специальный факультет СБ Украины ВИТИ НТУУ "КПИ"

Анотація: **Проведено аналіз стану відомчої системи радіозв'язку з рухомими об'єктами. За результатами аналізу зроблено висновок про необхідність її модернізації з використанням сучасних та перспективних технологій: широкополосних сигналів з псевдовипадковою перестройкою робочої частоти, спектрально ефективних видів модуляції, турбокодів та адаптивного контуру. Поставлено задачі, які необхідно вирішити для реалізації запропонованих напрямків модернізації відомчої системи радіозв'язку з рухомими об'єктами.**
Summary: **In the article the analysis of the state of the department system of radio contact is conducted with mobile objects. As a result of analysis a conclusion is done about the necessity of its modernization with the use of modern and perspective technologies after directions of the use of wideband signals with frequency hopping spread spectrum, spectral effective types of modulation, turbocodes and adaptive to the contour. The put tasks which it is necessary to decide for realization of the offered directions of modernization of the department system of radio contact with mobile objects.**
Ключові слова: **Відомча система радіозв'язку з рухомими об'єктами, широкосмугові сигнали, спектрально ефективна модуляція, турбокоди, адаптивний контур**.

I Введение

В соответствии со ст. 17 Конституции Украины обеспечение информационной безопасности государства является одной из его важнейших функций. Неотъемлемой составной частью организации информационной безопасности служит обеспечение защищенного информационного обмена в интересах управления государством, так как свыше 80% информации, передаваемой должностными лицами органов государственной власти Украины, составляет информация с ограниченным доступом [1, 2].

Одной из наиболее важных и сложных в ведомственной системе связи является ведомственная система радиосвязи с подвижными объектами (ВСРСПО). Она предназначена для обеспечения радиосвязью абонентов, которые находятся на подвижных объектах, как между собой, так и с абонентами других сетей связи. ВСРСПО была разработана в начале 70-х годов прошлого столетия и представляет собой комплекс дуплексной аналогово-цифровой связи с автоматическим поиском свободного канала. В Украине такая система была развёрнута в 1972 году.

В настоящее время большое количество работ как отечественных, так и зарубежных авторов посвящено анализу эффективности систем подвижной радиосвязи [3 – 6]. Анализ научно-технической политики в развитых странах свидетельствует о том, что главная её направленность проявляется во всё большей ориентации на использование новых информационных технологий, под которыми понимают совокупность методов, способов и средств сбора, накопления, сохранения, обработки и предоставления информации. Они базируются на новых достижениях в области прикладной информатики, которая объединяет информатику, вычислительную технику и автоматизацию. Толчком к стремительному развитию современных информационных технологий стали достижения последних десятилетий в областях микроэлектроники, вычислительной техники, оптических и квантовых технологий. Это дало возможность создать принципиально новые средства обработки, передачи и хранения информации.