рынках. Одной из причин такого положения является доступность к информации предприятия, выпускающего конкурентную продукцию. Одним из путей выхода из такой ситуации могли бы стать мероприятия, направленные на усиление информационной безопасности предприятия, т.е. на защиту информации [1]. Защита информации на любом предприятии может быть представлена в виде трех уровней:

1. Защита от конкурентов технико-экономических показателей выпускаемой продукции или научно-исследовательских и опытно-конструкторских разработок, в особенности в перспективных направлениях.

2. Защита внутренней текущей информации предприятия, в том числе данных о себестоимости продукции, складских запасах, наличии технических проблем.

3. Защита информации или данных, которые в том или ином виде присутствуют в выпускаемых изделиях.

Первых два уровня относятся к организационно-техническим мерам обеспечения безопасности, и их реализация сводится в основном к следующим действиям [1]:

- организация пропускного режима и службы безопасности,
- отбор работников при приеме на работу,
- заключение контрактов с работниками, в которых отражается ответственность за передачу информации третьим лицам,
- защита информации в локальной вычислительной сети (ЛВС) предприятия; введение в штат сотрудников, отвечающих за безопасность информации внутри сети.

К третьему уровню защиты информации может относиться защита технологии изготовления изделия (например, микросхемы), которая может быть восстановлена при анализе изделия, а также защита информации, хранящейся в самом изделии. Примером изделий, содержащих нуждающуюся в защите информацию, являются выпускаемые НИРУП "ЦНИИТУ" электронные пластиковые карты (ЭПК). В настоящее время НИРУП "ЦНИИТУ" постоянно наращивает выпуск телефонных ЭПК, освоена первая опытная партия банковских ЭПК, планируется освоение ЭПК для других применений — в качестве пропусков для проходных, автостоянок, для автоматизации выдачи зарплаты на предприятиях и т.д. Важнейшим техническим показателем и необходимым условием востребованности на рынке для телефонных ЭПК является защищенность их от несанкционированной перезарядки, для банковских ЭПК — их защищенность от несанкционированного доступа к содержащимся в ЭПК платежным ресурсам. По данному показателю ЭПК НИРУП "ЦНИИТУ" соответствуют современному научно-техническому уровню [2].

Литература

1. Тимченко И.М. Организационно-технические меры обеспечения комплексной безопасности предприятия: методология, специальные технические средства//Конспект лекций научно-практического семинара для руководителей предприятий Министерства промышленности Республики Беларусь по теме: "Обеспечение безопасности хозяйственной деятельности предприятия в рыночных условиях" (Минск, 18-19 февраля 2003 года). - Мн.: Институт экономики НАНБ, 2003. – С. 45-49.

2. Вечер Д.В., Прибыльский А.В., Реуцкий В.С., Таболич Т.Г. Сравнение кристаллов пластиковых карт по степени защиты информации//В этом сборнике. – С.

ЗАЩИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТРАНЫ ПРИ РЕГУЛИРОВАНИИ ИНТЕЛЛЕКТУАЛЬНОЙ МИГРАЦИИ

М.В. АЗАРЕНКО, А.Г. ПАЦЕЕВА

Организация защиты информации предполагает наличие целого комплекса разноцелевых разработок, повышающих эффективность управления не только техническими процессами, но и человеческими факторами. С формальной стороны человеческие отношения и в этой области регулируются правовыми нормами, например, законом РБ "О государственных секретах". Законодательство РБ предусматривает защиту большого набора разнообразных видов тайн, которые объединяются общей категорией — конфиденциальностью [1]. Разрабатываются основные организационные принципы защиты информационных ресурсов страны.

При такой разработке целесообразно учесть один из важных источников утечки информации - миграцию научных кадров [2]. Действительно, основными создателями научного и научно-технического информационного продукта являются научные кадры. Результаты научной деятельности, как правило, принадлежат ученому или научному коллективу, их создавшему. В свою очередь, государство заинтересовано в том, чтобы практическая реализация этих результатов осуществлялась в пределах страны, где информационный продукт был создан. Правовое регулирование вопросов собственности на ту или иную информацию заложено в патентном праве. С другой стороны, большое количество информации, идей, разработок, технологических нововведений до официального оформления прав собственности принадлежат их создателям. В силу того, что человек считает более выгодным для себя реализовать свои инновации и права на них в условиях другой страны, эти информационные ресурсы теряются для стран-доноров. Для стран с переходной экономикой, какой является Республика Беларусь, это создаёт проблемную ситуацию — чем интереснее разработки ученого для мировой науки или для иностранных компаний, тем выше вероятность того, что он уедет в другую страну, с более благоприятными социально-экономическим условиями. Страна в этом случае терпит не только информационные, но и прямые

экономические убытки. Для прекращения утечки информации за рубеж путем научной миграции кадров в республике в настоящее время не существует надежных правовых и организационных норм.

Поэтому для глубокой проработки вопроса об информационной безопасности страны с учетом влияния человеческого фактора при миграции кадров необходимо создание временных коллективов разработчиков названных норм. В этот коллектив обязательно должны войти специалисты по вопросам защиты информации Государственного центра защиты информации, Комитета государственной безопасности, Министерства труда и социальной защиты, Государственного Таможенного Комитета, аппарата Совета Министров, Национальной Академии Наук Беларуси, министерства образования и других заинтересованных государственных органов управления и науки. Дополнить коллектив могли бы специалисты Центра мониторинга миграции научных кадров при НАН Беларуси, изучающего миграцию на постоянное место жительства и выезд по долгосрочным контрактам за рубеж.

Результатом работы такого коллектива могло бы стать создание правовой базы и организационных структур для государственного регулирования интеллектуальной миграции в части защиты информационных ресурсов страны. В дальнейшем данной работой могли бы заниматься научные организации в области защиты информации.

Литература

1. Азаренко М.В. Организация защиты государственных секретов в государственных организациях в соответствии с белорусским законодательством // Конспект лекций научно-практического семинара для руководителей предприятий Министерства промышленности Республики Беларусь по теме: "Обеспечение безопасности хозяйственной деятельности предприятия в рыночных условиях" (Минск, 18–19 февраля 2003 года). Мн.: Институт экономики НАНБ, 2003.
2. Мирская Е.З. Современные телекоммуникационные технологии в Российской академической науке // Науковедение. 2000. № 3. С. 48–56.