

организации вне зависимости от сферы деятельности. Исходя из этого, общие положения по инвентаризации ресурсов, порядок ведения учета ресурсов, правила формирования реестра информационных ресурсов, порядок сбора, анализа, пересмотра и контроля учетной информации об информационных ресурсах должны определяться внутренней организационно-распорядительной документацией организации.

Таким образом, инвентаризация ресурсов определяет важные сведения, необходимые для обеспечения информационной безопасности автоматизированных информационных систем. А как известно, построение эффективной системы информационной безопасности является одним из наиболее важных условий успешного функционирования любой ИТ-инфраструктуры, что в свою очередь становится критическим фактором успешного ведения бизнеса.

Литература:

1. ISO/IEC 17799:2005 «Информационная технология. Методики безопасности. Практическое руководство для информационного управления безопасностью»;
2. www.iso27000.ru;
3. www.itsec.ru.

ОСОБЕННОСТИ ТРАНСФЕРА РЕЗУЛЬТАТОВ НАУЧНО-ТЕХНИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ ВУЗА, СОДЕРЖАЩИХ ОБЪЕКТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

О. ПУГАЧЕВА,

Гомельский госуниверситет им. Ф. Скорины (Республика Беларусь)

In article features of a transfer of results of scientific and technical activity of the high school, containing objects of intellectual property are considered, and also the general algorithm of protection of not opened information is resulted

Вузовский сектор Республики Беларусь, обладающий значительным научно-техническим и инновационным потенциалом, играет важную роль в создании экономики инновационного типа. Практика показывает, что новая модель университета как учебно-научно-инновационного комплекса, сочетающего академическую науку с развитой сетью высокотехнологичных инновационных структур и малых предприятий, является одним из наиболее эффективных базовых элементов национальной инновационной системы.

Развитию инновационной деятельности в регионе способствует создание в Гомельском госуниверситете им. Ф.Скорины опытно-промышленных производств абразивного инструмента и полирующих суспензий для полировки пластин полупроводниковых и других материалов, договора на производство и поставку которых

заключены с предприятиями города, Республики Беларусь и России. Созданные в 20 научно-исследовательских лабораториях наукоемкие и конкурентоспособные разработки неизменно вызывают интерес на различных выставках, становятся основой для последующих контактов и переговоров (таблица 1).

Таблица 1

Участие университета в выставках

Годы	Количество выставок, в которых участвовали учреждение и подразделения				Количество экспонатов, демонстрировавшихся на выставке							Количество и стоимость совершенных сделок (контракты, договора, соглашения)			
	в с е г о	в том числе			в с е г о	из них			в том числе			в с е г о	в том числе		
		РБ	РФ	Дальнее зарубежье		Нагур. образцы	планшеты	Компьют. техн. и прог. средства	РБ	РФ	Дальнее зарубежье		РБ	РФ	Дальнее зарубежье
2005	16	6	2	8	35	3	2	30	35	24	26	-	-	-	-
2006	17	5	5	11	37	1	2	34	37	30	25	5	1	2	2
2007	17	5	4	8	31	9	3	19	31	25	16	2	-	-	2
2008	17	5	5	4	27	12	3	12	27	23	16	2	-	-	2
2009	16	3	5	8	27	12	3	12	27	23	16	2	-	-	2
2010	14	5	3	6	30	10	4	16	30	23	16	7	1	3	3

В университете функционирует Центр коллективного пользования по экологическому мониторингу и исследованию состава и свойств вещества, способствующий продвижению в реальный сектор экономики разработок, выполненных на основе научных исследований в области технологий микро - и наноразмерных систем, физики и химии полимеров, спектрометрического анализа и исследования экосистем. Университет внедряет результаты научно-технической деятельности в производство и в учебный процесс (таблица 2).

Таблица 2

Использование научных разработок университета

Годы	Использование научных разработок		
	в народном хозяйстве	в учебном процессе	
		акты внедрения	издание монографий, учебников и учебных пособий
2005	12	64	320
2006	6	25	197
2007	-	131	256
2008	7	96	214
2009	6	131	157
2010	15	275	153

Анализ состояния и развития системы управления инновационной деятельностью в университете в 2005-2010 годах показывает стабильный рост основных показателей оценки результатов научно-технической и творческой деятельности, что связано с достаточно работоспособной системой управления инновационными процессами в вузе. Об этом также свидетельствуют данные, характеризующие число поданных заявок и полученных патентах на объекты промышленной собственности (таблица 3).

Таблица 3

**Сведения о поданных заявках и полученных патентах
на объекты промышленной собственности (ОПС)**

Годы	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
Количество поданных заявок	4	9	7	8	11	14	10	3	9	7	11
Количество полученных патентов	9	9	2	15	7	8	19	21	11	9	4

Трансфер технологий накладывает на его участников определенные обязательства, связанные со знанием норм и правил общения с объектами интеллектуальной собственности (объектами авторского права и ОПС), а также с практическими навыками их применения в конкретных ситуациях. Важным элементом успешного осуществления научно-технической деятельности вуза является охрана нераскрытой (конфиденциальной информации) или коммерческой тайны.

Основными каналами утечки сведений, содержащих коммерческую тайну, являются: любые формы сотрудничества; партнеры по совместным работам; экспонирование на отечественных и зарубежных выставках и иные формы рекламы; передача документации и образцов устройств, веществ, компьютерных программ, ноу-хау, результатов НИОКР партнерам; публикации в отечественных и зарубежных изданиях; договоры о выполнении НИОКР, договоры подряда; участие в конференциях и семинарах в стране и за рубежом; участие в конкурсах на получение грантов от иностранных и отечественных фондов; деятельность сотрудников вузов или иных научных организаций в качестве сотрудников или консультантов иностранных или отечественных исследовательских центров и предприятий; пребывание в лабораториях вуза специалистов зарубежных фирм, в том числе командированных, стажеров, аспирантов и студентов; предоставление сведений о лучших разработках вузов по запросам различных министерств, ведомств, ассоциаций, фирм, предприятий, фондов; плохая организация учета, хранения и прохождения документов, образцов, других носителей информации; обиженные сотрудники и др.

Общий алгоритм защиты нераскрытой информации может быть сведен к следующему: определение объекта защиты; выявление угроз и оценка их вероятности; оценка возможного ущерба; анализ эффективности применяемых мер защиты (физическая безопасность документации, надежность персонала, безопасность используемых для передачи информации каналов связи); определение

необходимых мер защиты (организационных, финансовых, юридических); внедрение дополнительно принятых мер защиты с учетом установленных приоритетов, доведение до персонала организации реализуемых мер, осуществление контроля; мониторинг и корректировка внедренных мер целью анализа работоспособности созданной системы безопасности информации.

МЕТОД ВЫЯВЛЕНИЯ ИНСАЙДЕРСКОЙ ДЕЯТЕЛЬНОСТИ

С. КАВУН, И. СОРБАТ,

Харьковский национальный экономический университет (Украина)

Актуальность. Предприятия и организации, банковские и финансовые учреждения, IT-компании разных стран Европы, США, России и Украины несут огромные финансовые потери вследствие экономической преступности и халатности сотрудников организаций, так называемой инсайдерской деятельности. Следовательно, возникает необходимость решения актуальной задачи выявления инсайдера или группы инсайдеров (инсайдерской деятельности), ответственных за утечку определенных категорий конфиденциальных данных в организации (на предприятии).

Над проблемами в данной сфере работают многие известные специалисты и ученые: Верин В.П., Гуров М.П., Олейников Е. А., Кизим М.О., Куркин Н.В., Шкарлет С.Н., Кавун С.В. и др. [1-8] В их работах были исследованы вопросы систематического подхода для устранения угроз информационной и экономической безопасности, но в большей части эти исследования касаются внешних угроз. Не до конца решенным остается вопрос внутренних угроз, и, как следствие, вопрос выявления (обнаружения) инсайдеров.

Целью статьи является представление нового метода, который позволит решить задачу выявления инсайдеров (инсайдерской деятельности) в организации (на предприятии).

Основной материал. По результатам анализа отчетов аналитических компаний – предлагается разделить предприятия и организации, в которых произошли обнародованные утечки на три категории: государственные учреждения, коммерческие предприятия, а так же учебные заведения и общественные не коммерческие структуры, для которых рассчитаны распределения источников утечек по видам организаций (табл. 1).

Для определения наиболее важных данных, подвергшихся утечке, выделено три основные категории конфиденциальной информации: персональные данные, государственная и коммерческая тайны. Подавляющее число инцидентов (90-98%) за весь период наблюдений охватывают персональные данные, что затрудняет выделение тенденций. Также получены распределения утечек по типам конфиденциальных данных (табл. 2).