

переменных:  $x_{10}, x_{11} = \text{целое}$ . Второе требование — сумма смен  $x_1-x_4$  должно быть равно  $x_{14}$ , а сумма  $x_5-x_{13} = x_{15}$ :  $x_{11}, x_{12} = x_{11}, x_{12}$ . Третье требование — на каждой смене количество официантов должно быть не менее указанного менеджером:  $x_{13}, x_{17} = x_{13}, x_{14}$ .

После выполнения поиска решения получим следующие результаты для заданной численности официантов (рис.2).

Требуется 21 человек, работающий на полную ставку и 8 человек, работающих 4 часа, что на 1 человека меньше, чем в настоящий момент работало на объекте исследования.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
8	$x_1$	$x_2$	$x_3$	$x_4$	$x_5$	$x_6$	$x_7$	$x_8$	$x_9$	$x_{10}$	$x_{11}$	$x_{12}$	$x_{13}$	$x_{14}$	$x_{15}$				
9	10-19	11-20	12-21	13-22	10-14	11-15	12-16	13-17	14-18	15-19	16-20	17-21	18-22	Полная	Неполная	Сумма произведений	Знак		
10	0	0	0	15	3	0	0	0	0	0	3	0	0	15	6				
11	1	1	1	1											-1	0	=	0	
12					1	1	1	1	1	1	1	1	1		-1	0	=	0	
13	1				1											3	>=	3	10-12
14	1	1	1	1				1								15	>=	15	13-15
15	1	1	1	1					1	1						15	>=	12	15-18
16		1	1	1							1	1	1			18	>=	18	18-20
17				1									1			15	>=	4	20-22
18														1	0,5	18	Min		

Рисунок 2 – Результаты решения задачи

Использование составленной программы и мониторинг требуемого количества официантов, работающих на сменах, позволит обеспечить повышение качества обслуживания.

УДК 004.056

## П. Захарченко

(Республика Беларусь)

Научный руководитель: Л.И. Крошинская, доцент  
БИП-Институт правоведения

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Современное развитие информационных технологий, и особенно Internet технологий, привело к возникновению острой необходимости защиты информации, передаваемой в сети открытого доступа. В связи с

этим возникает проблема надежного обеспечения защиты информации, которая передается и обрабатывается в информационно-вычислительных системах и сетях, а также безопасность самих систем и технологий.

Защита информации – комплекс правовых, организационных и технических мер, направленных на обеспечение целостности (неизменности), конфиденциальности, доступности и сохранности информации;

Информационная безопасность – это состояние защищенности национальных интересов в информационной сфере, которая является совокупностью интересов личности, общества и государства.

Основные составляющие информационной безопасности:

- доступность;
- целостность;
- конфиденциальность.

Доступность – это возможность за приемлемое время получить требуемую информационную услугу.

Целостность – защищенность информации от разрушения и несанкционированного изменения, а также актуальность непротиворечивость информации.

Конфиденциальность – это защита от несанкционированного доступа к информации.

Системы информационной безопасности должны уметь противостоять разнообразным атакам, как внешним, так и внутренним

Важность осуществления информационной безопасности объясняется следующими двумя основными причинами:

- ценностью накопленных информационных ресурсов;
- критической зависимостью от информационных технологий.

Потеря важной информации, кража конфиденциальных данных, перебой в работе вследствие отказа, проблемы с системами управления или медицинскими системами – все это может вылиться не только в крупные материальные потери, нанести ущерб репутации организации, а также могут стать угрозой здоровью и жизни людей.

Современные информационные системы, даже без учета активности злоумышленников, сложны и опасны уже сами по себе. Большой проблемой являются новые уязвимые места в программном обеспечении, которые обнаруживаются в процессе эксплуатации этих программ.

Успех в области информационной безопасности может принести только комплексный подход, состоящий из четырех уровней:

- законодательный;
- административный;
- процедурный;
- программно-технический.

Законодательный уровень является важнейшим для обеспечения информационной безопасности.

Без законодательной базы, без постоянного внимания руководства организации и выделения необходимых ресурсов, без мер управления персоналом и защиты решить ее невозможно.

Законодательство об информации, информатизации и защите информации в Республике Беларусь основывается на Конституции Республики Беларусь и состоит из Закона Республики Беларусь «Об информации, информатизации и защите информации» (10 ноября 2008 г. № 455-З), Указа Президента Республики Беларусь от 09 ноября 2010 г. №575 «Об утверждении Концепции национальной безопасности Республики Беларусь», иных актов законодательства Республики Беларусь.

Меры административного уровня – сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Основой программы мер административного уровня является политика безопасности, направленная на защиту информационных активов организации.

Процедурный уровень ориентирован на людей (а не на технические средства) и включает:

- управление персоналом;
- физическую защиту;
- поддержание работоспособности систем;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.
- проверка стратегии.

Меры безопасности целесообразно разделить на следующие виды:

- препятствующие нарушениям информационной безопасности (превентивные);
- меры обнаружения нарушений;
- сужающие зону воздействия нарушений;
- меры по выявлению нарушителя;
- меры восстановления режима безопасности.

В продуманной архитектуре информационной безопасности все они должны присутствовать.

Вследствие быстрого прогресса информационных технологий появляются дополнительные возможности не только у специалистов по информационной безопасности, но и у злоумышленников.

При обеспечении информационной безопасности успех может быть эффективным только при применении комплексного подхода.