Гончаренко Т.П. Информационная составляющая финансовой безопасности бизнеса / Т.П. Гончаренко, Н.О. Сидоренко // Информационные технологии в экономике, бизнесе и управлении : мат. Междунар. заоч. науч.-практ. конф. (20 февраля 2014 г.) / отв. ред. М. В. Старцев; М-во обр. и науки РФ. - Тамбов : Изд. Дом ТГУ им. Г. М. Державина, 2014. - С.29-34.

ИНФОРМАЦИОННАЯ СОСТАВЛЯЮЩАЯ ФИНАНСОВОЙ БЕЗОПАСНОСТИ БИЗНЕСА

Гончаренко Т.П., Сидоренко Н.О.
Государственное высшее учебное заведение «Украинская Академия банковского дела», г. Сумы, Украина
Харьковский региональный институт государственного управления Национальной академии государственного управления при Президенте Украины, г. Харьков, Украина

В условиях глобализирующихся экономик, интенсификации развития прогресса науки, техники и технологий, особенно в сфере коммуникаций, на первый план выходят вопросы, связанные с общим управлением информационными ресурсами, их безопасностью, а также взаимосвязью финансовой безопасности и степенью защищенности информации о финансовом состоянии организации, а также персональных данных физических лиц.

Широкое использование различных информационных технологий в бизнесе, начиная от документооборота, использования программного обеспечения и оканчивая торговлей он-лайн и безналичными расчетами, вызывают широкое обсуждение не только в среде практикующих управленцев, экспертов, чиновников, но и в научных кругах.

Понятие *«информационная технология»* может рассматриваться как совокупность средств и методов сбора, обработки и передачи данных (первичной информации) для получения информации нового качества о состоянии объекта, процесса или явления (информационного продукта) [2, с. 8].

На сегодняшний день существуют различные виды информационных технологий, например: *информационная технология обработки данных; информационная технология управления; автоматизация офиса; информационная технология поддержки принятия решений; информационная технология экспертных систем* [1].

Развитие современных информационных технологий способствовало использованию информационной составляющей для увеличения финансовой стабильности практически всеми структурными подразделениями и служащими любого предприятия. Например, юридические и кадровые службы постоянно отслеживают изменения нормативно-правого характера, тоже касается бухгалтерии и специалистов по оптимизации налогообложения. Отделы снабжения и сбыта, подразделения маркетинга и логистики отвечают за сбор и обработку больших массивов информации про тенденции макроэкономического развития экономики; рынкам; новациям; конкурентам и т.п. Практически на всех предприятиях возникла необходимость найма ИТ-специалистов, которые должны обеспечивать не только работу персональных компьютеров сотрудников, официальных сайтов компаний, систем управления, но также – информационную безопасность.

В зависимости от источников формирования и «ценности» информационных потоков субъекты хозяйственной деятельности могут классифицировать их следующим образом:

- открытая официальная информация;
- достоверная несекретная информация, м.б. получена неофициально (контакты сотрудников с носителями такой информации);
- конфиденциальная информация (представляет наибольшую ценность для финансовой стабильности предприятия) [3].

В современных условиях, именно информационная составляющая становиться основной для достижения финансовой стабильности бизнеса. Поэтому, для обеспечения её безопасности нужно учитывать способы обмена информационными технологиями, которые характерны для бизнеса (Рис.1).

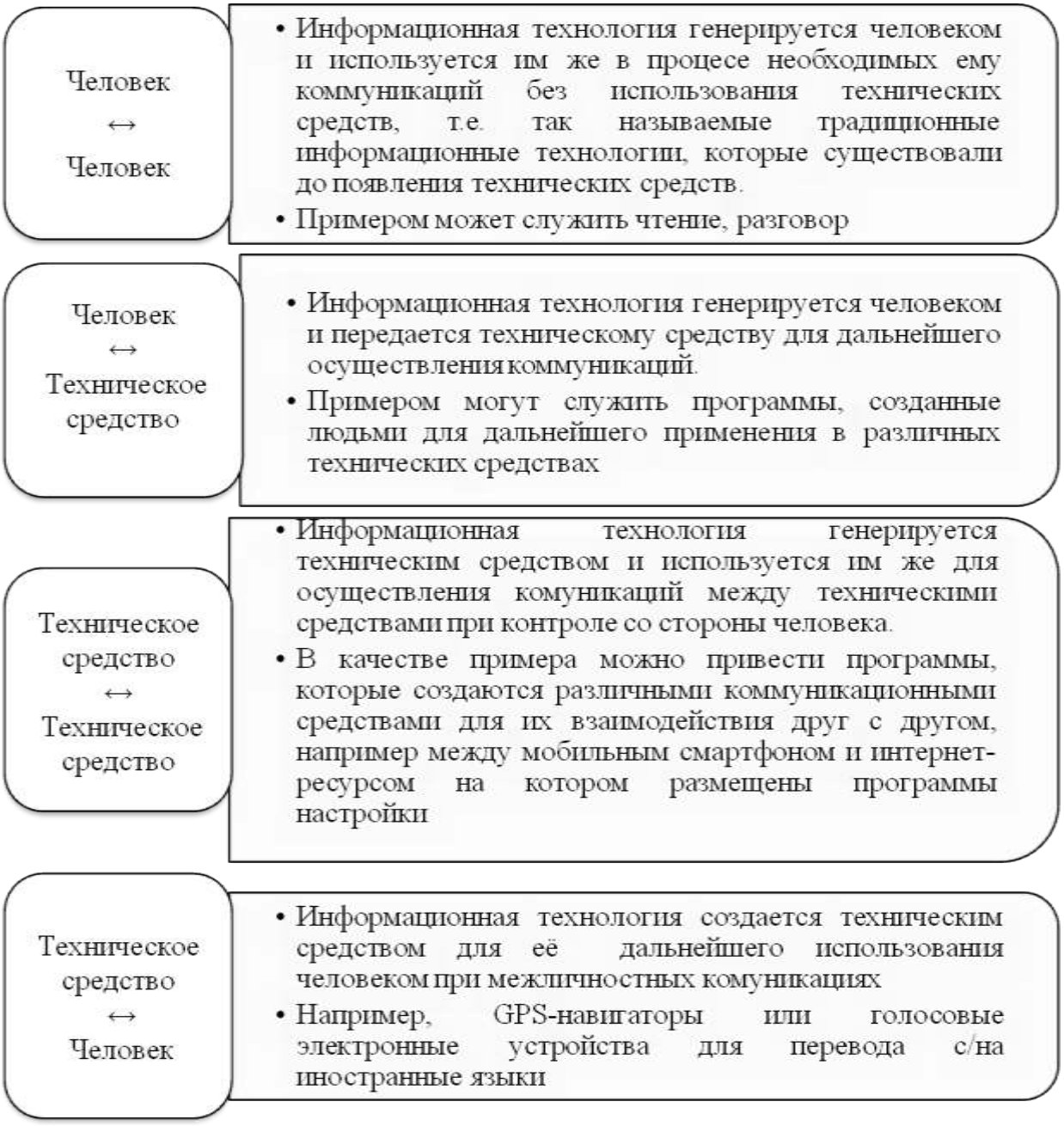

Рис. 1. Способы обмена информационными технологиями

С точки зрения обеспечения безопасности информации о финансовом состоянии бизнес-структуры, муниципального образования или персональных данных про физическое лицо, на наш взгляд достаточно уязвимыми являются пути передачи информации от человека к человеку.

В 2013 году нами было опрошено 50 руководителей различных бизнес-структур Сумской области на предмет того, насколько они обеспокоены вопросом сохранности информации на уровне межличностных коммуникаций. Абсолютно все руководители заявили о том, что они не уверены в том, что их сотрудники не передают информацию во внешнюю среду. При этом 82% руководителей, считают, что уровень оплаты труда абсолютно не влияет на этот процесс; 10% опрошенных полагают, что высокая заработная плата и социальное обеспечение сотрудников на высшем уровне может гарантировать защиту информации; 8% – не смогли определиться с ответом.

Важным моментом является также, тот факт, что все руководители озабочены возможностью утечки информации и хотели бы иметь реальный инструмент влияния на межличностные коммуникации, использование которого гарантировало бы им сохранность важной информации.

Следует отметить, что в последние годы внимание исследователей в основном было сосредоточено на необходимости создания защитных технологий применительно к хранению, защите и передаче данных, которые генерируются, хранятся и используются с помощью самых разнообразных технических средств. В то же время вопросу обеспечения безопасности информации при межличностных коммуникациях уделялось, на наш, взгляд не достаточно внимания.

Разрешение данной управленческой задачи лежит в плоскости мотивационных аспектов, а также формировании системы ценностей персонала сфокусированной на личной ответственности работников. В условиях современного уровня развития техники и технологий передачи данных, защита внутрисистемной информации приобретает несколько иной оттенок, что связано с многократно увеличившимся количеством способов, как анонимной передачи данных, так и авторской.

Источниками угроз информации являются люди, аппаратные и программные средства, используемые при разработке и эксплуатации автоматизированных систем (далее – АС), факторы внешней среды. Угрозы безопасности, порождаемые данными источниками можно разделить на два класса: непреднамеренные и преднамеренные.

Непреднамеренные угрозы связаны со стихийными бедствиями, сбоями и отказами аппаратно-программных средств. Реализация этих угроз приводит, как правило, к нарушению достоверности и сохранности информации в АС, реже – к нарушению конфиденциальности, однако при этом могут создаваться предпосылки для злоумышленного воздействия на информацию.

Преднамеренные угрозы связаны с незаконными действиями посторонних лиц и персонала АС. В общем случае в зависимости от статуса по отношению к АС злоумышленником может быть: разработчик АС, пользователь, постороннее лицо или специалисты, обслуживающие эти системы, а это

означает, что именно человек является ключевым звеном играющим роль в обеспечении безопасности информации.

Вопрос обеспечения сохранности информации о финансовом и иных состояниях бизнес-структур является чрезвычайно важным. Разглашение, преднамеренное или не преднамеренное, целенаправленная или случайная передача подобного рода информации способна привести организацию к различного рода кризисным состояниям, начиная от отклонения намеченных целей или же до их полной недостижимости. Утечка или разглашение любой конфиденциальной информация о финансовом обеспечении организации: наличии займов/кредитов, долгах, инвестициях, акционерах, договорных обязательств, технологиях, клиентах – может повлиять на стоимость ее акций, решение партнеров, кредиторов или клиентов о дальнейшем сотрудничестве и т.п.

Решение данной проблемы, может служить опыт японских компаний, а именно система мотивации, при которой сотрудник должен воспринимать организацию с точки зрения того, чтобезопасность организации гарантирует и его личную безопасность, что может быть достигнуто путем гарантирования пожизненного найма, при соблюдении определенных внутриорганизационных ном, правил и традиций. Пожизненный найм, на наш взгляд, должен стимулировать персонал к заботе о стабильности функционирования организации как источнике дохода и благосостояния. При этом в организациях должен соблюдаться принцип честности в отношении равных прав в возможности осуществлять карьерный рост, что в японском менеджменте является обязательным.

Американская модель ведения бизнеса, в отличии от Японской, для обеспечения финансовой безопасности предприятий использует как материальное стимулирование (акции или партнерство, карьера, социальное обеспечение) так и правовое регулирование (договора о неразглашении информации).

На наш взгляд, решение о том, какая информация и в каких объемах может быть передана во внешнюю среду, должна быть строго регламентирована внутриорганизационными решениями.

В этой связи, нам видится необходимым решение на любом предприятии таких задач как:

- *организация безопасности информации;*
- *меры наказания за утечку информации;*
- *меры стимулирующие неразглашение информации;*
- *соблюдение прав интеллектуальной собственности;*
- *контроль над сохранностью информации в объемах и качестве.*

Таким образом, решение вопроса о стимулировании персонала к защите внутрифирменной информации способно серьезным образом повлиять на общеэкономический уровень развития организации, ее финансовую безопасность.

Список использованных источников

1. Информатика: Учебник/ Под ред. Н.В. Макаровой. – М. : Финансы и статистика, 2002. – 768 с.
2. Шатунова О.В. Информационные технологии: Учебное пособие / О.В. Шатунова. – Елабуга : Изд-во ЕГПУ, 2007. – 77 с.
3. Экономика предприятия: Учебник / Под общ. ред. д-ра екон. наук, проф. С. Ф. Покропивного. – Пер. с укр. 2-го перераб. и доп. изд. – К. : КНЭУ, 2003. — 608 с.

Аннотация

Вопрос обеспечения сохранности информации о финансовом и иных состояниях бизнес-структур является чрезвычайно важным. Разглашение, преднамеренное или не преднамеренное, целенаправленная или случайная передача подобного рода информации способна привести организацию к различного рода кризисным состояниям, начиная от отклонения намеченных целей или же до их полной недостижимости. В этой связи важными являются вопросы организации безопасности информации, стимулирование и наказание за сохранность/разглашение информации и контроль над ее сохранностью.