
Теория и практика управления

УДК 658(005.934)

КАНАЛЫ УТЕЧКИ ЭКОНОМИЧЕСКОЙ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ

Гончаренко Ю.Ю.

Рассматривается понятие информационной экономической системы как инструмента управления предприятием, некоторые аспекты сохранения коммерческой тайны, дается краткая характеристика основных каналов утечки информации.

Ключевые слова: предприятие, информация, информационная экономическая система, канал утечки информации.

Обеспечение коммерческой тайны предприятия – одна из постоянно существующих проблем, которая сопровождает всю его деятельность: от момента возникновения до ликвидации [1]. Эта проблема не является чем-то постоянным даже в пределах одной фирмы, а представляет собой динамическую субстанцию, зависящую от множества внутренних и внешних факторов, включающих и подготовку персонала, и оснащение его всем необходимым арсеналом технических средств [2]. Сохранение коммерческой тайны является одной из составляющих успеха деятельности предприятия. Эта проблема имеет много аспектов, один из которых – своевременное выявление каналов утечки информации из информационных экономических систем предприятия [3]. Сложность этого аспекта характеризуется рядом противоречивых факторов. С одной стороны, сохранение тайны требует минимизации числа сотрудников, в том числе и из руководящего состава, имеющих доступ ко всем материалам и нюансам коммерческой деятельности [4], а с другой – наибольший успех достигается при условии, когда все члены трудового коллектива знают, что и зачем они делают, и какая часть от общей прибыли предприятия идет в их доход, заработную плату, премию и т.п. [5]. Использование электронных средств обработки информации значительно сократило время и облегчило документооборот как внутри самих предприятий, так и во внешних звеньях связей с поставщиками, потребителями, с государственными контролирующими структурами (налоговой инспекцией, казначейством, санитарной службой и др.) [6]. В то же время любые персональные электронные средства обработки и передачи информации имеют возможность выхода в Интернет и передачи в реальном масштабе времени достаточно большого объема данных [7]. Не достаточно иметь самые современные и защищенные информационно-коммуникационные системы передачи и обработки данных, если их обслуживают слабо подготовленные или недисциплинированные сотрудники, способные осуществить их копирование и вынос за пределы охранной зоны предприятия [8].

Зная возможные каналы утечки информации, можно грамотно организовать профилактическую предупредительную работу по обеспечению сохранения коммерческой тайны предприятия.

Целью данной работы является определение потенциально возможных каналов утечки информации из экономических информационных систем предприятия. Для достижения поставленной цели необходимо решить следующие научные задачи. Первоначально проанализировать структуру, состав, принципы построения информационных систем и особенности экономических информационных систем, затем дать характеристику возможных каналов утечки информации из экономических информационных систем.

Информационные системы включают в себя функциональные компоненты, компоненты системы обработки данных, организационные компоненты. Функциональные компоненты представляют собой подсистемы обработки информационных ориентиров по определенному функциональному признаку. Например, система регистрации и учета входящей и исходящей переписки, система данных персонала учреждения, система гидрометеорологических данных по маршрутам следования транспортных средств бухгалтерского учета и т.п. Другими словами, это специализи-

рованные подсистемы, входящие в единый информационный комплекс предприятия, если он существует. В ряде случаев каждая из выше приведенных информационных систем может функционировать самостоятельно, решая поставленные перед ней задачи. Для компонент системы обработки данных типовыми, как правило, являются следующие задачи: сбор и перенос информации на машинные носители (жесткий диск, гибкий диск), передача информации в места ее хранения и обработка, ввод информации в ЭВМ и контроль ввода, создание и ведение внутри машинной информационной базы, обработка информации на ЭВМ (накопление, сортировка, корректировка, выборка, арифметическая и логическая обработка), вывод информации, управление вычислительными процессами в вычислительных сетях.

Организационные компоненты информационной системы – это совокупность методов и средств для совершенствования организации ее функционирования. Сейчас эту компоненту принято называть информационными технологиями. Строго говоря, информационные технологии – это целенаправленный процесс преобразования информации, использующий совокупность средств и методов сбора, обработки, хранения и передачи информации. Как и многие другие технологии, информационная технология должна отвечать следующим требованиям. Во-первых, обеспечивать высокую степень деления всего процесса обработки информации на составляющие компоненты (фазы, этапы, операции, действия). Во-вторых, включать весь набор инструментов, необходимых для достижения поставленной цели. В-третьих, отдельные компоненты должны быть стандартизированы и унифицированы. Информационная система также может рассматриваться как коммуникационная система по сбору, передаче и обработке информации об объекте, снабжающая работников различного ранга информацией для реализации функций управления. В общем виде система охватывает комплекс взаимосвязанных элементов, действующих как единое целое в интересах цели. Каждая система обладает свойствами делимости и целостности. В первом случае систему можно представить как структуру, состоящую из относительно самостоятельных частей (подсистем), каждая из которых может рассматриваться как система. Это упрощает анализ, разработку, внедрение и эксплуатацию. Свойство целостности указывает на согласование целей функционирования всей системы с целями функций ее подсистем и элементов. Каждая информационная система создается для конкретного объекта. Она должна принимать во внимание различие между уровнями управления, сферами действий, а также внешними обстоятельствами и давать каждому уровню управления только ту информацию, которая ему необходима для эффективной реализации функций управления. Внедрение информационных систем позволяет повысить эффективность производственно-хозяйственной деятельности не только за счет обработки и хранения информации, но и за счет применения новых методов управления, основанных на моделировании действий специалистов фирмы при принятии решения и использовании методов искусственного интеллекта.

Экономические информационные системы обеспечивают управление специфическими процессами на предприятии, такими как бухгалтерский учет и отчетность, технико-экономическое планирование, бизнес-план и т.д. Здесь также присутствует информация о производстве, распределении, обмене и потреблении материальных благ. Для этой экономической информации характерны простые алгоритмы, преобладание арифметических операций, табличное представление входных и выходных данных. Важнейшими методологическими принципами построения экономической информационной системы являются: системный подход, когда каждое событие рассматривается как составная часть общего процесса или явления; разработка с учетом возможности пополнения и обновления функций и состава без нарушения ее функционирования; наличие информационных интерфейсов, благодаря которым она может взаимодействовать с другими системами в соответствии с установленными правилами; модульная структура построения программного и информационного обеспечения, а также использование принципа единой информационной базы, чтобы исходная информация, один раз воспринятая и введенная в ЭВМ, могла быть использована многократно. Исходя из вышеизложенной структуры экономической информационной системы, в ней возможны следующие каналы утечки информации – это акустический, акусто-электрический и телефонный каналы

Акустический канал утечки информации реализуется различными способами. Во-первых, подслушивание разговоров на открытых площадках (балконах, верандах, курилках и т.п.) и в помещениях, находясь рядом или используя направленные микрофоны, которые бывают параболическими, трубчатыми или плоскими. Их направленность не более 5° градусов, а средняя дальность действия наиболее распространенных – трубчатых, составляет около 100 м. При хороших климатических условиях на открытой местности параболический направленный микрофон может работать на расстоянии до 1 км. Негласная запись разговоров может осуществляться на диктофон или магнитофон, а также подслушивание разговоров с использованием выносных микрофонов, так называемых радиозакладных устройств (дальность действия радиомикрофонов 50-200 м без ретрансляторов). Микрофоны, используемые в радиозакладках, могут быть встроенными или выносными. Они могут быть двух типов: акустическими, чувствительными в основном к действию звуковых колебаний воздуха и предназначенными для перехвата речевых сообщений, и вибрационными, преобразующими в электрические сигналы колебания, возникающие в разнообразных жестких конструкциях.

Особенностями акустоэлектрического канала утечки информации являются удобство применения (электросеть есть везде), отсутствие проблем с питанием у микрофона и возможность съема информации с питающей сети, не подключаясь к ней (используя электромагнитное излучение сети электропитания). Прием информации от таких «жучков» осуществляется специальными приемниками, подключаемыми к силовой сети в радиусе до 300 м от «жучка» по длине проводки или до силового трансформатора, обслуживающего здание или комплекс зданий.

Телефонный канал утечки информации используется для подслушивания телефонных переговоров. Возможен гальванический съем телефонных переговоров (путем контактного подключения подслушивающих устройств в любом месте абонентской телефонной сети). Он определяется путем ухудшения слышимости и появления помех, а также с помощью специальной аппаратуры. Возможен съем информации телефонно-локационным способом (путем высокочастотного навязывания), при этом по телефонной линии подается высокочастотный тональный сигнал, который воздействует на нелинейные элементы телефонного аппарата (диоды, транзисторы, микросхемы), на которые тоже воздействует акустический сигнал, в результате чего в телефонной линии формируется высокочастотный модулированный сигнал. Обнаружить подслушивание возможно по наличию высокочастотного сигнала в телефонной линии. Однако дальность действия такой системы из-за затухания ВЧ-сигнала в двухпроводной линии не превышает 100 м. Противодействие возможно путем подавления в телефонной линии высокочастотного сигнала. Применяются также индуктивный и емкостной способы негласного съема телефонных переговоров (бесконтактное подключение). Индуктивный способ состоит в использовании свойств электромагнитной индукции, возникающей в процессе телефонных переговоров вдоль провода телефонной линии. В качестве приемного устройства съема информации используется трансформатор, первичная обмотка которого охватывает один или два провода телефонной линии. Емкостной способ основан на формировании на обкладках конденсатора электростатического поля, изменяющегося в соответствии с изменением уровня телефонных переговоров. В качестве приемника съема телефонных переговоров используется емкостной датчик, выполненный в виде двух пластин, плотно прилегающих к проводам телефонной линии.

Подслушивание разговоров в помещении с помощью телефонных аппаратов возможно с использованием низкочастотного и высокочастотного способов съема акустических сигналов с телефонных переговоров. Данные способы основаны на подключении к телефонной линии подслушивающих устройств, которые передают преобразованные микрофоном звуковые сигналы по телефонной линии на высокой или низкой частоте, что позволяет прослушивать разговор как при поднятой, так и при опущенной телефонной трубке. Защита осуществляется путем отсекания в телефонной линии высокочастотной и низкочастотной составляющей. Возможно также использование телефонных дистанционных подслушивающих устройств, которое основывается на установке дистанционного подслушивающего устройства в элементы абонентской телефонной сети путем параллельного подключения его к телефонной линии с дистанционным включением. Дис-

танционное телефонное подслушивающее устройство имеет два демаскирующих свойства: во-первых, в момент подслушивания телефонный аппарат абонента отключен от телефонной линии, во-вторых, даже при положенной телефонной трубке и включенном подслушивающем устройстве напряжение питания телефонной линии составляет менее 20 Вольт, в то время как она должно составлять 60.

ВЫВОДЫ

Таким образом, для сохранения коммерческой тайны необходимо во всех служебных помещениях предприятия, в первую очередь там, где функционирует экономическая информационная система, организовать работу по выявлению и локализации возможных каналов утечки информации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Савицкая Г.В. Анализ хозяйственной деятельности предприятия / Г.В. Савицкая. – М.: МГУ, 2010. – 282 с.
2. Шеремет А.Д. Управленческий учет / А.Д. Шеремет. – М.: МГУ, 2010. – 240 с.
3. Лошкарёв В.Г. Организация бизнеса с нуля. / В.Г. Лошкарёв – М.: Изд-во РИА, 2010. – 204 с.
4. Введение в современную информатику / [М.М. Дивизинюк, Б.С. Бусыгин, Г.М. Коротенко и др.]. – Севастополь: СКУЭИП, 2005. – 392 с.
5. Методи керування інформаційною безпекою / [Ю.Ю. Гончаренко, М.М. Дивизинюк, В.О. Хорошко та ін.]. – Севастополь: СКУЭИП, 2010. – 328 с.
6. Типизация моделей технологических решений провайдинга Интернет / [М.М. Дивизинюк, Е.В. Азаренко, С.С. Азаров и др.]. – Севастополь: СКУЭИП, 2005. – 112 с.
7. Проектирование систем технической защиты информации / [Ю.Ю. Гончаренко, М.М. Дивизинюк, И.Н. Павлов и др.]. – Севастополь: СКУЭИП, 2011. – 235 с.
8. Герасимов Б.М. Системы піддержки прийняття рішень / Б.М. Герасимов, М.М. Дивизинюк, И.Ю. Субач. – Севастополь: Гос. океанариум, 2004. – 318 с.

УДК 681.3

МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК СОСТАВНАЯ ЧАСТЬ ДЕЯТЕЛЬНОСТИ РУКОВОДИТЕЛЯ ПРЕДПРИЯТИЯ

Ожиганова М.И.

Анализируются теоретические аспекты возможного ущерба при потере коммерческой и технологической информации, а также оптимальные затраты на предотвращение таких потерь. Рассматриваются вопросы информационной безопасности в повседневной деятельности руководителя предприятия.

Ключевые слова: предприятие, менеджмент, информация, информационная безопасность, руководитель предприятия.

Обеспечение безопасности информации, циркулирующей на предприятиях, а также между предприятиями и государственными учреждениями – одна из составных частей информационной безопасности государства, в частности, и национальной безопасности государства в целом [1]. Исходя из этого менеджмент информационной безопасности является актуальной научной задачей, решение которой осуществляется и компетентными государственными структурами, и руководителями предприятий различных форм собственности, выполняющими государственные заказы [2].