МЕНЕДЖМЕНТ

УДК 65.012.45

А.В. Балановская*

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ ПРОМЫШЛЕННОСТИ

В статье рассматриваются подходы к определению сущности информационной безопасности, проблемы ее обеспечения на предприятиях в современных условиях. Выделяются задачи и уровни обеспечения информационной безопасности промышленных предприятий. Подробно исследуется основные характеристики информации, обеспечивающие информационную безопасность.

Ключевые слова: информационная безопасность, защита информации, информационные угрозы, информационная система, конфиденциальная информация.

В настоящее время возрастает зависимость промышленных предприятий от значительного объема информационных потоков. С развитием информационных и коммуникационных технологий произошло изменение в области обмена различными видами информации между субъектами, что позволяет при помощи информационных технологий оперативно решать многие задачи современного общества. Тем не менее, постоянное усложнение вычислительных систем и сетей, в основе которых находятся внутриорганизационное, межорганизационное, национальные и мировое информационные пространства, ставит перед современным обществом задачу обеспечения информационной безопасности (ИБ). С каждым годом технологии защиты данных совершенствуются, однако уязвимость защиты не только не уменьшается, но и постоянно растет. Поэтому очевидна актуальность проблем, связанных с защитой потоков данных и информационной безопасностью, – их сбора, хранения, обработки и передачи.

На наш взгляд, информационная безопасность – это состояние защищенности любой информации, не только обрабатываемой в информационно-компьютерных системах. Ведь компьютерная техника является только частью информационной системы. Но, в то же время, большее внимание всегда сосредоточивается на защите информации, передаваемой с помощью компьютеров.

Балановская Анна Вячеславовна (balanovskay@mail.ru), кафедра экономики промышленности Самарского государственного экономического университета, 443086, Российская Федерация, г. Самара, ул. Советской Армии, 141.

В качестве общенаучной категории безопасность можно определить как такое состояние рассматриваемой системы, когда она способна противостоять влиянию внешних и внутренних угроз, а функционирование этой системы не создает угрозы для ее составляющих, а также внешней среды [1].

Это состояние наиболее эффективного использования информационно-технологического ресурса организации в целях укрепления финансово-экономической стабильности предприятия, защита конфиденциальной информации и коммерческой тайны предприятия, сбор и анализ информации как внутренней, так и внешней среды [2].

Отсюда следует вывод, что основой обеспечения ИБ является решение трех взаимосвязанных проблем: проблемы защиты информации, находящейся в системе, от влияния внутренних и внешних угроз; проблемы защиты информации от информационных угроз; проблемы защиты внешней среды от угроз со стороны находящейся в системе информации.

К настоящему времени достигнуты определенные результаты по теоретическому изучению и практической разработке проблемы ИБ, которая уже более 30 лет находится в центре внимания специалистов. Заложены основы теории защиты информации, разработаны разнообразные средства защиты информации и налажено их производство, накоплен опыт практического решения задач защиты информации в различных системах, разработана государственная система защиты информации. Проблема защиты информации имеет реальную основу для дальнейшего развития.

Понятие «информационная безопасность» используется в практической жизни и деятельности весьма широко. При этом даже специалисты вкладывают в это понятие различный смысл. Наиболее часто оно подменяется родственным понятием «защита информации», в результате чего проблема сводится к частной задаче защиты информации от утечки по различным физическим каналам при ее обработке средствами вычислительной техники.

Следует различать понятия «информационная безопасность» и «защита информации», которые в научной и учебной литературе зачастую отождествляются, что приводит к путанице. Нам представляется необходимым их разграничить. Защита информации представляет собой комплекс мер по обеспечению ИБ, т. е. это правовые, организационные, технические меры (способы, методы, средства, механизмы, действия) по предотвращению угроз ИБ и устранению их последствий. К основным элементам защиты информации мы относим: создание условий, ограничивающих распространение информации; предупреждение несанкционированного доступа к информации; предотвращение хищения, утечки, искажения, уничтожения, разглашения информации; обеспечение права собственника на владение и распоряжение информацией и т. д.

Обеспечение информационной безопасности представляет собой сложную и многогранную проблему. Она должна обеспечиваться для всех экономических агентов и хозяйствующих субъектов, т. е. населения – основного носителя информации, предприятий и организаций, а также для государства в целом. Определим, прежде всего, задачи и уровни обеспечения ИБ, включающие в себя заинтересованные в ИБ субъекты (рис. 1).

Задачи ИБ состоят в том, чтобы обеспечить четыре основные характеристики информации, а именно: доступность, целостность, конфиденциальность и достоверность. Под этими терминами принято понимать соответственно: способность систем представлять своевременный беспрепятственный доступ к информационным ресурсам субъектов, обладающих соответствующими правами; защиту от сбоев,

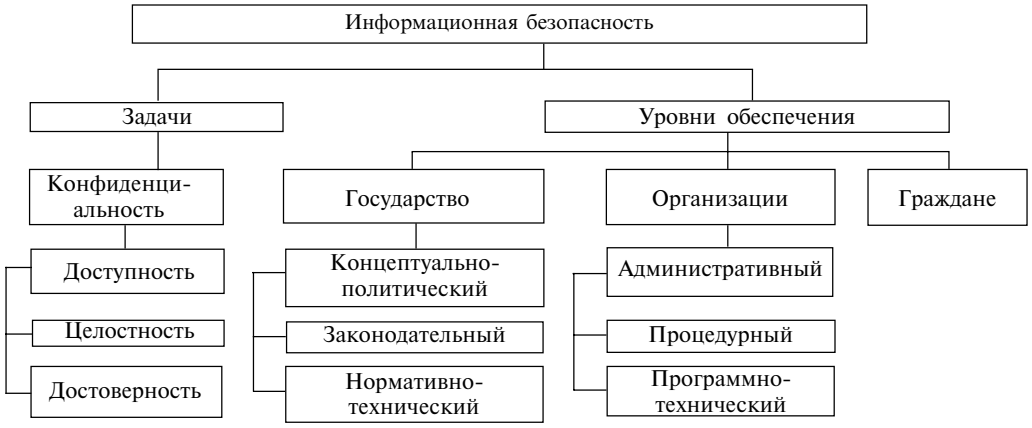

Рис. 1. Задачи и уровни информационной безопасности

ведущих к потере информации, защиту от несанкционированных изменений или уничтожения данных; ограниченный доступ к информации, предназначенной только для авторизированного пользователя; общую полноту и точность воспринимаемой информации.

Наиболее важным и сложным для реализации на практике аспектом ИБ является обеспечение ее конфиденциальности. Существуют три основные причины, приводящие к потере конфиденциальности информации: разглашение, утечка и несанкционированный доступ (рис. 2).

Рис. 2. Причины потери конфиденциальности информации

Под разглашением понимается событие, приведшее в результате преднамеренных или неумышленных действий к получению информации субъектами, не обладающими соответствующими правами. Разглашение может осуществляться различными способами. Это могут быть сообщение, передача, пересылка, публикация, утеря и т. п. Осуществляется разглашение формальными и неформальными каналами предоставления информации. К формальным каналам следует отнести переговоры, деловые встречи, совещания и т. п. Неформальными каналами служат личные встречи, переписка, выставки, конференции, средства массовой информации

и т. п. Обычно разглашение конфиденциальной информации происходит в результате некомпетентности сотрудников, невыполнения правил защиты секретных сведений.

Под утечкой мы понимаем неконтролируемый процесс передачи конфиденциальной информации за пределы предприятия или определенного круга лиц. Утечка конфиденциальной информации происходит при помощи технических каналов. Каналом утечки информации называется физический путь конфиденциальных сведений, используя который злоумышленник может получить доступ к охраняемым информационным ресурсам. Каналы утечки информации классифицируются по способу переноса информации на материально-вещественные, акустические, визуально-оптические и электромагнитные.

Несанкционированным доступом называется преднамеренное действие, направленное на получение конфиденциальной информации лицом, не обладающим соответствующими правами доступа к ней. Осуществляется несанкционированный доступ при помощи различных методов, к которым относятся подкуп сотрудников, насильственное склонение к сотрудничеству, непосредственное проникновение на объект и др.

Условиями, способствующими неправомерному завладению конфиденциальной информацией, принято считать: подкуп, болтливость сотрудников, отсутствие контроля, отсутствие трудовой дисциплины, плохую работу кадровых служб при найме работников, психологическую несовместимость, низкую заработную плату и т. п.

Также одной из задач ИБ является обеспечение доступности информации, поскольку информационные системы (ИС) строятся и служат для предоставления различного рода информационных услуг (продуктов). Нарушение связи, отказ в доступе к получению подобных услуг влекут за собой значительный ущерб заинтересованных субъектов. Ведущая роль доступности проявляется в системах управления в различных сферах деятельности предприятий. В настоящее время в РФ доступностью информации на государственном уровне не занимается пока никто.

Отсутствуют аппаратно-программные продукты отечественной разработки общего назначения, повышающие доступность информационных систем.

Целостность информации как задача ИБ подразделяется на статическую и динамическую. Под статической целостностью понимается неизменность информационных ресурсов, динамическая же относится к точному проведению сложных операций – транзакций. Обеспечение динамической целостности информации важно при проведении финансовых операций с целью обнаружения краж, дублирования и т. п. Нарушение целостности информации, т. е. ее искажение, потеря, ошибки в различных областях человеческой деятельности могут привести к непредсказуемым результатам.

Перейдем к рассмотрению уровней обеспечения ИБ. На концептуально-политическом уровне принимаются документы, определяющие направления государственной политики информационной безопасности, формулируются цели и задачи, пути и средства их достижения.

На законодательном уровне создается и поддерживается комплекс мер, направленных на правовое регулирование и обеспечение ИБ, отражаемых в законах и других правовых актах (указы Президента, постановления Правительства и др.). Важнейшей задачей этого уровня выступает формирование механизма, позволяющего согласовать процесс разработки законов с прогрессом в области информационных технологий. К правовым мерам относятся действующие в стране законы, указы и другие нормативные правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информаци-

онных отношений в процессе ее получения, обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом. Эти меры в основном ориентированы на устранение искусственных угроз и являются базисом для реализации остальных мер.

На нормативно-техническом уровне разрабатываются стандарты, руководящие и методические материалы, а также другие документы, регламентирующие процессы разработки, внедрения и эксплуатации средств обеспечения ИБ. Одной из главных задач этого уровня является приведение российских стандартов к международным.

На уровне организации (предприятия) осуществляются конкретные меры по обеспечению ИБ. Их состав и содержание определяются особенностями конкретной организации или предприятия. В основе подобных мер лежит политика ИБ, представляющая собой совокупность документированных управленческих решений, целью которых является обеспечение защиты информации и связанных с ней ресурсов. Она определяет стратегию, необходимое количество средств и ресурсов, выделяемых организацией на обеспечение должной ИБ. Политика ИБ формируется на основе проведения анализа существующих рисков, угрожающих информационной системе предприятия.

К организационным относятся меры административного и процедурного характера, регламентирующие процессы функционирования ИС, использования ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей и обслуживающего персонала с ИС таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации. Сюда же следует отнести процедуры (механизмы) принятия решений по управлению ИБ, и в первую очередь – механизмы распределения ресурса, выделяемого на мероприятия по поддержанию и повышению ИБ.

На процедурном уровне определяются непосредственные меры по обеспечению ИБ, осуществляемые людьми. К ним можно отнести управление персоналом, физическую защиту и планирование восстановительных работ (рис. 3).

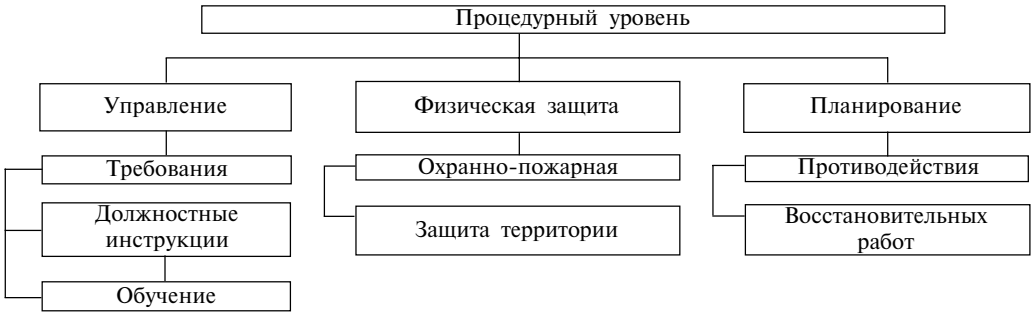

Рис. 3. Меры по обеспечению ИБ предприятия на процедурном уровне

На программно-техническом уровне осуществляется защита оборудования, программных средств и информационных ресурсов. Эти меры основаны на использовании различных устройств и специальных программ, входящих в состав ИС и выполняющих (самостоятельно или в комплексе с другими средствами) функции

защиты с целью устранения угроз, непосредственно связанных с процессом хранения, обработки и передачи информации.

Реализуется это при помощи сервисов безопасности (идентификация и аутентификация; разграничение доступа; протоколирование и аудит; шифрование; экранирование; обеспечение целостности; обеспечение доступности; обеспечение отказоустойчивости).

При всем существующем на сегодняшний день богатстве выбора программно-технических решений обеспечить ИБ предприятия на этом уровне до сих пор остается непростой задачей. Причиной этого служит стремительное развитие информационных технологий по следующим направлениям: повышение быстродействия систем; развитие сетевых технологий и рост их пропускной способности; значительный рост программных продуктов, созданных в сжатые сроки и не защищенных должным образом в связи с высокой конкуренцией на рынке и погоней за прибылью; создание и развитие новых информационных сервисов.

Технические меры основаны на применении разного рода механических, электро- и электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также средств визуального наблюдения, связи и охранной сигнализации. Также можно выделить инженерно-технические меры, связанные с оптимизацией построения зданий, сооружений, сетей инженерных коммуникаций, транспортных магистралей и т. д., с учетом требований ИБ.

Чрезвычайно важным остается правовой аспект обеспечения ИБ, связанный с необходимостью совершенствования законодательной базы в этой сфере. Нормативно-правовая база обеспечения ИБ не охватывает всего круга проблем в этой области, а в отдельных вопросах противоречива. Ситуация осложняется тем, что российские информационные технологии сильно отстают от мировых стандартов, слабо развита отечественная индустрия средств информатизации, телекоммуникаций и связи, затруднен выход российской продукции на мировые рынки. Решение вышеназванных проблем позволит создать наукоемкие технологии, осуществить технологическое перевооружение промышленности, приумножить достижения отечественной науки и техники.

Организационные меры играют ключевую роль в обеспечении ИБ ИС. Организационные меры – это единственное, что остается, когда другие методы и средства защиты отсутствуют или не могут обеспечить требуемый уровень ИБ. Организационные меры необходимы для эффективного применения других мер в части, касающейся регламентации деятельности людей. В то же время организационные меры необходимо поддерживать экономическими, инженерно-техническими, техническими и программно-аппаратными средствами.

Библиографический список

1. Стрельцов А.А. Обеспечение информационной безопасности России: теоретические и методологические основы. М.: Издательство Московского центра непрерывного математического образования (МЦПМО), 2002. 296 с.

2. Кастельс М. Информационная эпоха: экономика, общество и культура / пер. с англ. под научн. ред. О.И. Шкартана. М.: ГУ ВШЭ, 2000. 268 с.

A.V. Balanovskaya*

MAINTENANCE OF INFORMATION SECURITY OF THE INDUSTRIAL ENTERPRISES

Approaches to the definition of essence of information security, a problem of its maintenance at the enterprises in modern conditions are considered. Problems and levels of maintenance of information security of the industrial enterprises are allocated. The basic characteristics of information, providing information security are investigated in more detail.

Key words: information security, information protection, information threats, information system, confidential information.

* *Balanovskaya Anna Vyacheslavovna* (balanovskay@mail.ru), the Dept. of Industrial Economics, Samara State University of Economics, Samara, 443086, Russian Federation.