Геращенко Маужида Мидехатовна
канд. пед. наук, доцент
Мягков Вадим Вячеславович
студент
Сибирский институт управления (филиал)
ФГБОУ ВО «Российская академия народного хозяйства
и государственной службы при Президенте РФ»
г. Новосибирск, Новосибирская область

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ

Аннотация: *в статье рассматривается информация как особая ценность для бизнеса. Обеспечение защиты информации, торговых марок, авторских прав и других объектов интеллектуальной собственности способствует эффективному развитию компаний и получению стабильных доходов. Авторы приводят множество разнообразных методов и средств для защиты информации.*

Ключевые слова: *информационная безопасность, коммерческая организация, защита информации.*

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных:

– на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий;

– на соблюдение конфиденциальности информации ограниченного доступа;

– на реализацию права на доступ к информации [1, статья 16].

В сферу повышенного интереса конкурирующих компаний входит конфиденциальная для бизнеса информация, а, именно сведения о деятельности и менеджменте предприятия. Несанкционированный доступ к конфиденциальной

информации и ее изменение могут нанести существенный урон финансовому положению коммерческой организации. При этом, информационная утечка может быть даже частичной. В некоторых случаях обеспечение хищения 20% конфиденциальной информации может иметь критические последствия для экономической безопасности компании [2]. Основными причинами утечки информации при отсутствии должного обеспечения информационной безопасности в организации становятся различные случайности, вызванные неопытностью сотрудников. А случайности очень сложно предсказывать, соответственно, и противодействовать им почти невозможно.

Рассмотрим основные понятия. Итак, безопасность информации – это создание условий, исключающих доступ для просмотра, модерации и уничтожения данных субъектами без наличия соответствующих прав и обеспечивающих защиту от утечки и кражи информации с помощью современных технологий и инновационных устройств. Защита информации – это полный комплекс мер по обеспечению целостности и конфиденциальности информации при условии ее доступности для пользователей, имеющих соответствующие права. Целостность – это сохранность качества информации и ее свойств. Конфиденциальность – это обеспечение секретности данных и доступа к определенной информации отдельным пользователям. Доступность – это возможность быстрого и точного нахождения информации конкретными пользователями [2].

Следовательно, важнейшей целью защиты информации нужно считать минимизацию ущерба вследствие нарушения требований целостности, конфиденциальности и доступности.

В настоящее время существуют несколько угроз информационной безопасности коммерческой организации. К ним можно отнести неблагоприятную экономическую политику государства, когда оно осуществляет регулирование экономикой при помощи манипуляций, (например, учетная ставка, налоговые ставки, таможенные тарифы), которые создают множество противоречий на предприятиях в их производственной и финансовой сферах. Политические дей-

ствия государства, направленные на ограничение или прекращение экономических связей, вызывают у обеих сторон недоверие к дальнейшей деятельности и подрывают коммерческие взаимоотношения. Кроме этого, серьезную опасность представляют действия других хозяйствующих субъектов. В данном случае риск обеспечению безопасности информации несет нездоровая конкуренция (например, попытка представить потребителю деятельность одной коммерческой структуры под видом другой; дискредитирование репутации коммерческого предприятия путем распространения ложной информации; неправомерное и некорректное использование торговых обозначений, вводящих потребителя в заблуждение; экономическое подавление, которое выражается в разных формах – шантаж персонала, руководителей, компрометирующая информация, парализация деятельности предприятия, срыв сделок с помощью медиаканалов, коррупционных связей в госорганах). Не следует забывать и о кризисных явлениях в мировой экономике. Кризисы имеют особенность перетекать из одной страны в другую, используя каналы внешних экономических связей. Это следует учитывать, определяя методы и средства обеспечения информационной безопасности организации. Поэтапное интегрирование России в международную экономику способствует зависимости коммерческих предприятий страны от различных процессов, происходящих в мировой экономике (падение и рост цен на энергоносители, структурная перестройка и так далее).

Итак, современное производство в стремлении к увеличению прибыли, улучшению деятельности путем модернизации, повышению уровня обеспечения безопасности информации обязательно должно обращать внимание на мировую политику, внешнюю и внутреннюю политику государства и центрального банка, развитие научно-технического прогресса, отношения конкурентов, динамику потребительского спроса.

Система безопасности потенциальных и реальных угроз непостоянна, поскольку те могут появляться, исчезать, уменьшаться или нарастать. На основании этого система обеспечения информационной безопасности организации рас-

сматривается как целый комплекс принятых управленческих решений, направленных на выявление и предотвращение внешних и внутренних угроз. Эффективность принятых мер основывается на определении таких факторов, как степень и характер угрозы, аналитическая оценка кризисной ситуации и рассматривание других неблагоприятных моментов, представляющих опасность для развития предприятия и достижения поставленных целей [2]. Система информационной безопасности предприятия должна включать в себя:

– компьютерную безопасность, которая обеспечит качественную работу всех аппаратных компьютерных систем и создаст единый целостный, конфиденциальный и доступный ресурс;

– безопасность коммуникаций, которая предотвратит доступность информации, выданной по телекоммуникационному запросу, неавторизированным субъектам;

– безопасное программное обеспечение, которое включает комплекс общецелевых и прикладных программ, направленных на безопасную обработку всех данных и безопасную работу всех систем;

– безопасность данных, которая защитит информацию от случайных, халатных, неавторизированных и умышленных разглашений или взлома системы.

Базой для обеспечения информационной безопасности организации служит принятие следующих мер: анализ реальных и потенциально возможных ситуаций, представляющих угрозу безопасности информации, оценка характера угроз, принятие комплекса мер для определения угрозы и реализация принятых мер по предотвращению угрозы.

Основная цель обеспечения комплексной системы безопасности информации для защиты предприятия – это создание благоприятных условий для нормального функционирования в условиях нестабильной среды; обеспечение защиты собственной безопасности; возможность на законную защиту собственных интересов от противоправных действий конкурентов; обеспечение сотрудников сохранностью жизни и здоровья; предотвращение возможностей материального и финансового хищения, искажения, разглашения и утечки конфиденциальной

информации, растраты, производственных нарушений, уничтожения имущества и обеспечение нормальной производственной деятельности [3].

Эффективная система обеспечения информационной безопасности организации должна основываться на следующих принципах:

– принцип комплексности, то есть при создании систем защиты информации должна быть учтена вероятность возникновения всех возможных угроз для конкретной организации. Используемые средства защиты должны совпадать с вероятными видами угроз и функционировать комплексно, дополняя друг друга технически;

– принцип непрерывности, то есть работа всех систем безопасности должна быть непрерывной и круглосуточной;

– принцип надежности, то есть все зоны безопасности должны иметь одинаковую степень надежной защиты;

– принцип эшелонирования, то есть обеспечение информационной безопасности организации будет осуществляться в таком порядке, при котором все зоны системы защиты информации будут располагаться последовательно, а самая важная из них будет располагаться внутри всей системы;

– принцип разумной достаточности, то есть применение защитных средств должно быть разумным без попыток создания «абсолютной защиты». Нужно понимать, что эффективные системы защиты информации очень дорогие, поэтому к их выбору необходимо подходить рационально. Стоимость защитной системы не должна превышать размер возможного ущерба и затраты на ее обслуживание и функционирование.

В настоящее время для обеспечения защиты информации используют множество разнообразных методов и средств. Рассмотрим основные из них:

– препятствие – это защита информации при помощи запрета на доступ к аппаратуре и информационным носителям с использованием простой физической силы в виде внешней охраны или специальных электронных устройств, таких как электронная пропускная система, система наблюдения, система пожар-

ной безопасности, замковая система, система микровыключателей, фиксирующая открывание дверей и окон, защитные наклейки, посылающие сигнал тревоги при попытке выноса и так далее;

– управление доступом – это использование регулирующих ресурсов системы, предотвращающих несанкционированный доступ к информационным носителям при помощи присвоения каждому объекту и пользователю личного идентификатора, аутентификации по заявленному идентификатору, проверки соответствия полномочий для выполнения заявленных процедур, регистрация всех обращений в виде протоколирования, немедленное реагирование на попытку несанкционированного доступа в виде задержки работ, отказа в запросе, отключения. Управление доступом осуществляется при помощи аппаратных средств защиты, то есть устройств, встроенных в блоки информационной автоматизированной системы и обеспечивающих запрет несанкционированного доступа, защиту файловых систем архивов и баз данных при любых сбоях в работе системы, защиту всех программ и приложений. Кроме этого, управление доступом осуществляется при помощи программных средств защиты, которые входят в состав программного обеспечения или являются элементами аппаратных систем защиты. Они обеспечивают безопасность информации при помощи реализации логических и интеллектуальных защитных функций, таких как контроль входа и загрузок при помощи логинов, паролей, кодов и тому подобное, обеспечение безопасности потоков конфиденциальной информации, защита от воздействия вирусного программного обеспечения, уничтожение остаточных данных конфиденциального характера в оперативной памяти, формирование протоколов об уничтожении, протоколирование данных о работе пользователей с подготовкой отчетов в регистрационном журнале системы;

– регламентация – это сведение к минимуму доступа к хранению и передаче данных при несанкционированном запросе;

– маскировка – это криптографическое закрытие, которое защищает доступ к информации в автоматизированной системе;

– принуждение – это обязательное соблюдение пользователями определенных правил при доступе к закрытой информации, приводящее при несоблюдении к различным мерам ответственности;

– побуждение – это соблюдение установленных правил на использование запрещенной информации, основанный на этических и моральных нормах.

Итак, в современных условиях информация имеет особую ценность для бизнеса. Обеспечение защиты информации, торговых марок, авторских прав и других объектов интеллектуальной собственности способствует эффективному развитию компаний и получению стабильных доходов.

Список литературы

1. Федеральный закон от 27.07.2006 года №149-ФЗ «Об информации, информационных технологиях и защите информации» (ред. от 19.12.2016) с изм. и доп., вступ. в силу с 01.01.2017 [Электронный ресурс]. – Режим доступа: consultant.ru

2. Обеспечение информационной безопасности организации [Электронный ресурс]. – Режим доступа: iccwbo.ru (дата обращения: 14.03.2017).

3. Хорев А.А. Цели и задачи защиты информации [Электронный ресурс]. – Режим доступа: sec.ru (дата обращения: 16.03.2017).