**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ОСНОВНОЙ ЭЛЕМЕНТ КОРПОРАТИВНОЙ КУЛЬТУРЫ ОРГАНИЗАЦИЙ ЭЛЕКТРОННОГО БИЗНЕСА**

Князькова Вероника Святославовна

г. Минск, Белорусский Государственной Университет

Информатики и Радиоэлектроники

Сегодня мы можем наблюдать интересное явление – переход от постиндустриального к информационному обществу. Этот переход затрагивает все сферы деятельности человека – технические, экономические, социальные и т.д. Перемены носят многоаспектный характер, меняя привычные нам паттерны и стратегии поведения как на микро-, так и на макроуровнях. Наиболее ярко данные изменения прослеживаются на примере электронного бизнеса (ЭБ). В международной практике бизнес признается электронным, если хотя бы две его составляющие из четырех (производство, маркетинг, логистика, расчеты) осуществляются с помощью сети Интернет.

На сегодняшний момент нет единого, устоявшегося определения электронного бизнеса. В данной статье автор будет опираться на определение ЭБ, данное Климченей Л.С.: «ЭБ представляет собой деловую активность с преобразованными бизнес-процессами за счет применения информационных технологий в целях обеспечения более высокой экономической эффективности деятельности» [1].

Технологии ЭБ позволяют организациям более эффективно и гибко управлять своими внутренними и внешними бизнес-процессами, что в свою очередь позволяет более тесно сотрудничать с поставщиками и партнерами, а также более полно удовлетворить ожидания своих клиентов.

В зависимости от целевой группы потребителей, классификация ЭБ осуществляется по следующим категориям [2]:

* [Бизнес для бизнеса (B2B)](http://www.financialguide.ru/encyclopedia/b2b)
* [Бизнес для потребителя (B2C)](http://www.financialguide.ru/encyclopedia/b2c)
* Бизнес для сотрудников (B2E)
* [Бизнес для правительства (B2G)](http://www.financialguide.ru/encyclopedia/b2g)
* [Правительство для бизнеса (G2B)](http://www.financialguide.ru/encyclopedia/g2b)
* Правительство для правительства (G2G)
* [Правительство для гражданина (G2C)](http://www.financialguide.ru/encyclopedia/g2c)
* Потребитель для потребителя (С2С)
* Потребитель для бизнеса (C2B)

К основным видам ЭБ относятся [2]:

* Торговые площадки (интернет-биржи, аукционы, каталоги товаров и услуг);
* Электронное управление закупками;
* Порталы (корпоративные, информационные, коммерческие, персональные);
* Организация, содержание и обслуживание общественных глобальных сетей (осуществляется операторами сетей);
* Финансовые услуги (интернет-платежные системы, обменные пункты, интернет-банкинг, [онлайн-трейдинг](http://www.financialguide.ru/encyclopedia/trading));
* Инвестиционные фонды (консолидированные инвестиционные фонды или буферные фонды и [паевые инвестиционные фонды](http://www.financialguide.ru/encyclopedia/paevoj-investicionnyj-fond));
* Интернет-магазины;
* Контент-проекты (сайты с бесплатной и востребованной информацией для привлечения посетителей с целью ведение рекламного бизнеса);
* Информационные посредники (каталоги, рейтинги, поисковые системы);
* Информационный бизнес в Интернете (периодические интернет–издательства, новостные сайты и т.д.);
* Интернет-маркетинг (продвижение сайта в поисковых системах);
* Рекламный бизнес;
* Услуги связи и средства общения;
* WEB-мастеринг (создание сайтов, веб-программирование, веб-дизайн, раскрутка сайтов);
* MLM или сетевой маркетинг (форма ведения внемагазинной розничной торговли);
* Разработка ПО и цифровых товаров;
* Услуги сервис-провайдеров (поставщики сетевых услуг, поставщики хостинга, доменов);
* Предоставление услуг (дистанционное обучение, сетевые библиотеки, электронное здравоохранение, интернет-консалтинг и т.д.);
* Игорный бизнес в сети (виртуальные казино, букмекерские конторы, тотализаторы, лотереи);
* Биржи труда (агентства по трудоустройству);
* Партнёрские программы (аффилат–программы и др.);
* Интернет-франчайзинг;
* Интернет-лизинг.

ЭБ, тесно связанный с сектором информационно-коммуникационных технологий, с телекоммуникациями и обменом всевозможной информацией (зачастую конфиденциального характера), представляет традиционному бизнесу как новые возможности, так и новые угрозы. Информация стала стоить гораздо дороже многих материальных ценностей, и ее потеря может поставить под угрозу существование самого бизнеса. В этой связи хотелось бы упомянуть базовый нормативно-правовой документ, дающий определения и устанавливающий основные цели и требования по защите информации в нашей стране – Закон Республики Беларусь «Об информации, информатизации и защите информации», принятый 10 ноября 2008 года № 455-З. В нем, в частности, содержится определение информации (информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления), а также цели защиты информации. К ним относятся:

* обеспечение национальной безопасности, суверенитета Республики Беларусь;
* сохранение и неразглашение информации о частной жизни физических лиц и персональных данных, содержащихся в информационных системах;
* обеспечение прав субъектов информационных отношений при создании, использовании и эксплуатации информационных систем и информационных сетей, использовании информационных технологий, а также формировании и использовании информационных ресурсов;
* недопущение неправомерного доступа, уничтожения, модификации (изменения), копирования, распространения и (или) предоставления информации, блокирования правомерного доступа к информации, а также иных неправомерных действий).

Принятие этого Закона означало огромный шаг вперед в области защиты информации, стало отправной точкой в разработке политик безопасности на всех уровнях управления. Разумеется, разработка политики безопасности и планов по совершенствованию корпоративной стратегии защиты информации для достижения приемлемого уровня защищенности информационных активов организации не является общим для всех процессом. Каждая отдельно взятая организация нуждается в индивидуальном решении. В развитии подходов к информационной безопасности организации сегодня главной тенденцией является переход от "заплаточных" систем, которые состоят из поставляемых разными производителями компонентов, обеспечивающих решение "узких" задач, к комплексным интегрированным системам информационной безопасности. Подобные системы позволяют организациям избавиться от возникающих при использовании "заплаточных" решений проблем, связанных с совместимостью компонентов, управлять всеми компонентами в рамках единой административной консоли, а также сокращать затраты на внедрение и сопровождение системы обеспечения информационной безопасности [3].

С технической точки зрения средства защиты информации можно условно разделить на следующие сегменты [4].

1. Межсетевые экраны. На сегодняшний день они являются основным средством обеспечения сетевой безопасности. Впервые они появились в конце 80-х годов. С их помощью решалась задача разделения компьютерных сетей. С тех пор принципиальных изменений эта технология практически не претерпела. На данный момент практически невозможно отыскать межсетевой экран без возможности организации VPN (VPN – англ. *Virtual Private Network* – виртуальная частная сеть; обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети). Интеграцию межсетевых экранов с антивирусами и средствами обнаружения атак тоже можно считать решенной задачей.

2. Средства построения VPN.В данном сегменте средств защиты основной задачей производителей является повышение производительности процессов шифрования. Этого требует рост телекоммуникационных возможностей. Второе направление, в котором развивается данная технология – «мобильность» клиента. Под этим понимается не только внедрение соответствующего функционала в карманные компьютеры, смартфоны и телефоны, но и создание клиентов, не требующих предварительной установки какого-либо софта. Такой клиент может загружаться как скрипт, например во время посещения защищенного раздела корпоративного сайта.

3. Антивирусы. Сегодня многие компании, издающие антивирусное программное обеспечение, предлагают комплекс средств для построения эшелонированной защиты: компоненты их систем не только защищают рабочие станции и сервера, но и закрывают наиболее вероятные пути проникновения вирусов в сеть – почтовые шлюзы и Proxy-сервера для доступа в Интернет.

4. Обнаружение атак. Сегодня наиболее часто используется DoS-атака (DoS расшифровывается как *Denial of Service* и дословно означает отказ в обслуживании; DoS-атака – это хакерская атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднён). В настоящий момент для предотвращения атак такого типа широко используется как программные, так и аппаратные средства защиты (например, Nginx – http сервер, который помимо прочего помогает снизить нагрузку на сервер вследствие множества запросов; Firewall – распространенный вид защиты, который существенно снижает эффективность DoS-атаки; распределение нагрузки – создание нескольких дополнительных, запасных серверов низкого уровня и отдельных каналов).

5. Контроль содержимого. Интерес к данному сегменту возникает, в частности, благодаря распространению спама. Тем не менее его основное предназначение состоит в предотвращение утечки конфиденциальной информации и пресечении нецелевого использования Интернета.

По мнению автора, достижение задачи создания комплексной системы управления безопасностью должно идти параллельно с встраиванием идеологии защиты информации в ДНК организации, в ее корпоративную культуру. Именно целостный, всесторонний подход позволит обеспечить информационную безопасность организаций ЭБ.

Существует множество подходов к определению понятия корпоративная (внутренняя, организационная) культура. Сведем основные из них в таблицу 1 [5].

Таблица 1. Основные определения понятия «корпоративная культура»

|  |  |
| --- | --- |
| Автор | Определение |
| Э. Джекс | Вошедший в привычку, ставший традицией образ мышления и способ действия, который в большей или меньшей степени разделяют все работники предприятия и который должен быть усвоен и хотя бы частично принят новичками, чтобы новые члены коллектива стали «своими». |
| Г. Хофстед | Организационную культуру можно определить как коллективное программирование мыслей, которое отличает членов одной организации от другой. Она является психологическим активом организации, который может быть использован для прогнозирования финансовых  результатов деятельности фирмы через пять лет. |
| А. Колос и Д. Репка | Организационная культура – это условная система, состоящая из набора правил и стандартов, определяющих взаимодействие и согласованность членов коллектива, управленческого звена, структурных подразделений и ключевых факторов развития предприятия. |
| Х. Шварц и С. Дэвис | Комплекс убеждений и ожиданий, разделяемый членами организации, эти убеждения и ожидания формируют нормы, которые в значительной степени определяют поведение в организации отдельных личностей и групп. |

Корпоративная культура базируется на ос­новополагающих ценностях, разделяемых членами организации. Эти ценности в разных организациях могут быть разными и в том числе зависеть от т.н. групп влияния (стейкхолдеров), представляющих собой физические и/или юридические лица, которые оказывают влияние (или на которых оказывает влияние) на деятельность организации.

В понятие корпоративной культуры входит корпоративное поведение, ставшее в последние годы объектом пристального изучения как теоретиков, так и практиков. Основные принципы кор­поративного поведения стали формулироваться в начале 1990-х гг. в т.н. кодексах корпоративного поведения. Пионерами здесь стали Англия, США и Канада. Изначально эти кодексы регулировали практику корпоративного поведения, в частности, вопросы обеспечения интересов акционеров, подот­четности директоров и руководства компанией. С тех пор во мно­гих странах изданы кодексы корпоративного поведения с соответ­ствующими методическими рекомендациями.

В Республике Беларусь Министерством финансов совместно с Министерством экономики, Государственным комитетом по имуществу и иными заинтересованными структурами был разработан Свод правил корпоративного поведения.
При подготовке свода правил были учтены нормы белорусского законодательства, а также принят во внимание международный опыт корпоративного поведения, в том числе Кодекс корпоративного поведения, разработанный Федеральной комиссией по рынку ценных бумаг России. Отметим, что целевая аудитория данного Свода правил – акционерные общества.

Положения белорусского свода правил базируются на признанных в международной практике принципах корпоративного управления, разработанных Организацией экономического сотрудничества и развития, в соответствии с которыми в последние годы рядом других государств были приняты кодексы корпоративного управления и аналогичные им документы [6].

Приказом Министерства финансов от 18.08.2007 г. № 293 акционерным обществам, созданным на территории Беларуси, рекомендовано следовать положениям свода правил. Подчеркивается, что применение акционерными обществами его положений является добровольным. Исходя из своей организационно-правовой формы, отраслевой принадлежности, структуры капитала и других особенностей, акционерное общество вправе использовать те рекомендации свода правил и в том объеме, которые оно сочтет для себя приемлемыми.

В своде правил приводится определение понятия «корпоративное поведение». Под ним понимают широкий термин, охватывающий систему отношений между органами управления и должностными лицами хозяйственного общества, владельцами ценных бумаг, а также другими заинтересованными лицами, так или иначе вовлеченными в управление обществом как юридическим лицом. С точки зрения тематики данной статьи особый интерес представляет глава 7 свода правил «Раскрытие информации об обществе». В ней указывается цель раскрытия информации об обществе: донесение информации до сведения всех заинтересованных в ее получении лиц в объеме, необходимом для принятия взвешенного решения об участии в обществе или совершении иных действий, способных повлиять на финансово-хозяйственную деятельность общества. Называются также и основные принципы раскрытия информации об обществе:

* регулярность и оперативность ее предоставления,
* доступность для большинства акционеров и иных заинтересованных лиц,
* достоверность и полнота ее содержания,
* соблюдение разумного баланса между открытостью общества и соблюдением его интересов.

Кроме того, в своде правил содержатся рекомендации по разработке Положения об информационной политике, в которое рекомендуется включать:

* изменение наименования общества;
* принятие решения об увеличении (уменьшении) уставного капитала;
* приобретение обществом собственных акций, если это не связано с уменьшением уставного капитала общества (при этом должна раскрываться информация об источниках средств, используемых для приобретения собственных акций, о количестве приобретаемых акций, цене приобретения, а также иная информация, раскрывающая причину и цели такого приобретения);
* повышение (понижение) цены акций общества не менее чем на 5 процентов;
* изменение приоритетных направлений деятельности общества;
* внесение в устав общества изменений, касающихся размещения привилегированных акций иного типа по сравнению с размещенными ранее;
* изменение депозитария эмитента.

Внимание также уделено и защите информации, составляющей коммерческую или служебную тайну. Указано, что информация составляет служебную или коммерческую тайну в случае, когда она представляет собой действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет доступа на законном основании и обладатель информации принимает меры по охране ее конфиденциальности.

В своде правил рекомендуется разработать локальный нормативный акт, утверждаемый руководителем общества (например, Положение об информации, составляющей коммерческую или служебную тайну), в котором был бы определен перечень такой информации об обществе, порядок ее защиты, а также порядок доступа к ней. Кроме того, указано, что в обществе должен осуществляться контроль за использованием инсайдерской (закрытой) информации.

В качестве примера рассмотрим УП «Велком», которое оказывает услуги мобильной связи под торговыми марками velcom и ПРИВЕТ на основе технологий GSM (GPRS, EDGE), UMTS (HSDPA, HSUPA), Dual-Carrier HSDPA на всей территории Беларуси, а также услуги фиксированного интернета на базе собственной оптоволоконной сети. УП «Велком» входит в состав Telecom Austria Group (TAG), одного из ведущих телекоммуникационных холдингов в Центральной и Восточной Европе, объединяющего восемь компаний-операторов фиксированной и мобильной связи. Можно сказать, что эта компания, входящая в сектор информационно-коммуникационных технологий, также участвует в электронном бизнесе.

Отметим высокую озабоченность УП «Велком» вопросами безопасности – как корпоративной, так и пользователей. Для них, к примеру, на сайте компании по адресу http://www.velcom.by создан раздел «Мобильная безопасность» с рекомендациями по безопасности для абонентов по направлениям защита от мошенничества, безопасный мобильный интернет, детям и их родителям.

Более подробно остановимся на Кодексе поведения компании [7]. Он состоит из шести разделов: 1) введение, 2) ценности Telecom Austria Group, 3) основные нормы поведения, 4) деловая этика в повседневной работе, 5) соблюдение стандартов поведения и 6) вопросы. Аспекты, связанные с обращением с информацией (защита и сохранность данных, сохранение конфиденциальности, обращение с внутренней информацией и информацией, относящейся к рынку капитала) находятся в четвертом разделе «Деловая этика в повседневной работе».

Рассмотрим вышеназванные аспекты более подробно. Компания утверждает, что она охраняет персональные данные и коммерческие тайны, которые становятся известны в результате ее деятельности. Для защиты конфиденциальной информации в компании разработаны и внедрены особые правила, процедуры и системы контроля.

*Защита данных.*Telecom Austria Group собирает и обрабатывает персональные данные только с разрешения вовлеченного лица, если это разрешено законом и необходимо для исполнения контрактных или правовых обязательств. Более того, компания собирает, обрабатывает и использует персональные данные только в необходимой степени и для заданных целей. Обработка всех данных осуществляется строго в рамках местного законодательства.

*Сохранность данных.*Сохранность данных имеет большое значение для Telekom Austria Group. Данный аспект существенно влияет на успешность бизнеса и репутацию компании. Поэтому в ней тщательно охраняется информация о компании, а так же личные данные клиентов и сотрудников, применяя все имеющиеся и подходящие технические и организационные средства для предотвращения несанкционированного доступа и использования или злоупотребления, потери и преждевременного уничтожения такого рода информации.

*Сохранение конфиденциальности.*Помимо технических средств и организационных мер, направленных на защиту информации, каждый из сотрудников обязан сохранять в тайне коммерческие и производственные секреты. Такая информация должна охраняться и может разглашаться только тем сотрудникам компании, которым ее необходимо знать для выполнения своих профессиональных обязанностей. Это также относится к информации, которую считают конфиденциальной деловые партнеры Telekom Austria Group, в особенности, если это оговорено в специальном соглашении о неразглашении.

При встречах или телефонном разговоре с коллегами в общественных местах сотрудники компании обязаны соблюдать конфиденциальность информации. Кроме того, посторонним лицам запрещено заглядывать в документы. Обязательство сохранять конфиденциальность остается в силе и после завершения трудоустройства в компании.

*Обращение с внутренней информацией и информацией, относящейся к рынку капитала.* Являясь компанией, чьи акции котируются на фондовой бирже, Telekom Austria AG обязана придерживаться строгих стандартов рынка капитала. В компании осознают, что злоупотребление внутренней информацией – приобретение и продажа ценных бумаг, будучи заранее осведомленным, в отличие от других участников рынка, а также раздача рекомендаций с использованием внутренней информации и распространение внутренней информации без производственной необходимости – запрещено и является уголовным преступлением. Любая информация, имеющая влияние на курс акций, является строго конфиденциальной. Ее можно распространять, только если на это есть производственная необходимость, подтвержденная документально.

*Финансовая целостность.* В пределах служебных обязанностей сотрудников компании они гарантируют целостность и верность созданных отчетов и документов, а также то, что каждая операция или расход отражены верно и проведены вовремя и в соответствии с существующими правилами и стандартами.

Таким образом, сегодня вопросы информационной безопасности являются основными для организаций любой отраслевой принадлежности. Особо важными они являются в электронном бизнесе. Для наиболее максимального проникновения методологии информационной безопасности в организацию эти вопросы следует интегрировать в корпоративную культуру и правила корпоративного поведения компании. На сегодняшний день в Беларуси уже имеются отлично зарекомендовавшие себя примеры такого проникновения. В статье был рассмотрен Кодекс поведения УП «Велком», изучив который можно сделать вывод о том, что интеграция корпоративной культуры, поведения организации и информационной безопасности в компании органично и целесообразно. Такой подход можно смело рекомендовать к использованию во всех организациях электронного бизнеса.

Литература

1. Климченя Л.С. Электронная коммерция: Учеб. пособие / Л.С. Климченя. – Мн.: Выш. Шк., 2004. С. 7.
2. http://www.financialguide.ru/encyclopedia/e-business.
3. Варакса Е. Защита информации – как часть системы корпоративной безопасности [Электронный ресурс]. Режим доступа: <http://searchinform.ru/press/articles/306/>
4. М. Савельев. Защита информации в корпоративных сетях // Мир связи. Connect! №9, 2004. [Электронный ресурс]. Режим доступа: <http://www.bre.ru/security/23293.html>
5. Шинкаренко О.Н. Корпоративная культура. Мифы и реальность // Кадры предприятия, №9, 2011. [Электронный ресурс]. Режим доступа: <http://dis.ru/library/571/27403/?sphrase_id=336773>
6. [http://news.tut.by/economics/93991.html](http://news.tut.by/economics/93991.html%2021.03.16)
7. <http://www.velcom.by/ru/documents/ru/Kodeks_Povedeniya.pdf>