УДК 65

Р.А. Ешенко,
канд. экон. наук, доцент кафедры информационных систем и технологий
Хабаровской государственной академии экономики и права
О.И. Чуйко,
канд. экон. наук, доцент кафедры информационных систем и технологий
Хабаровской государственной академии экономики и права

ЭКОНОМИЧЕСКАЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

Экономическая и информационная безопасность коммерческого предприятия заключается в защищенности интересов собственника данного предприятия, удовлетворяемых с помощью информации либо связанных с защитой от несанкционированного доступа тех сведений, которые представляются собственнику достаточно важными.

Ключевые слова: *экономическая и информационная безопасность, коммерческое предприятие, несанкционированный доступ.*

Economic and information security of commercial enterprise is to protect the interests of the owner of this enterprise. There interests are satisfied with the help of information or associated with protection of information important to the owner from unauthorized access.

Keywords: *economic and information security, commercial enterprise, unauthorized access.*

Экономическая и информационная безопасность коммерческого предприятия заключается в защищённости интересов собственника данного предприятия, удовлетворяемых с помощью информации либо связанных с защитой от несанкционированного доступа тех сведений, которые представляются собственнику достаточно важными [1]. По данным аналитического центра «InfoWatch» [4], актуальность вопроса защиты информации одинаково важна как для малого и среднего бизнеса, так и для крупного. В среднем финансовый показатель ущерба от утечки в расчёте на запись в среднем бизнесе даже выше, чем в крупном.

Если в крупных компаниях утечка одной записи о клиентах или сотрудниках (персональные данные, в том числе реквизиты пластиковых карт, номера соцстрахования и проч.) «стоит» 13,4 дол., в среднем бизнесе ущерб от утечки (на одну запись) составляет 15,9 дол. (рисунок 1) [4].

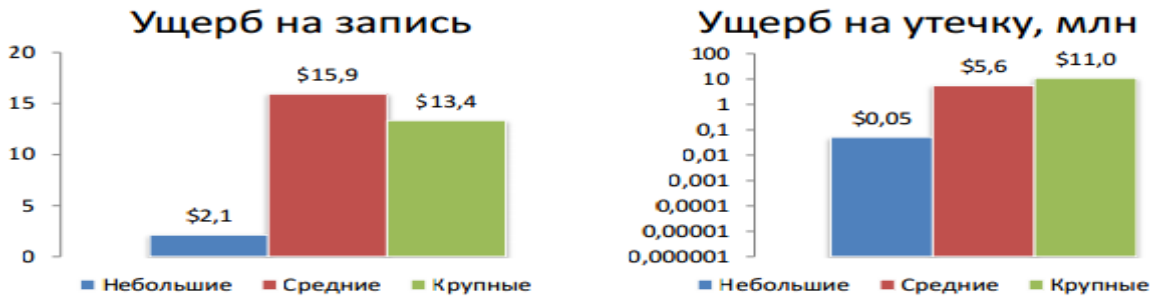

Рисунок 1 - Ущерб от утечки в расчёте на запись, на утечку, дол. США

Возникают основные вопросы при рассмотрении защиты бизнес-информации:

1. От чего следует защищать экономическую систему бизнеса?

2. Какие существуют риски и угрозы бизнесу?

3. С помощью каких методов и средств можно защитить информацию по бизнесу?

В бизнесе в первую очередь необходимо защищать следующую информацию [2]:

– тактику и стратегию развития компании;

– технологию работы бизнес-процессов;

– денежные и материальные потоки компании;

– новые продукты компании и технологии их изготовления.

Если рассматривать экономические показатели, темпы роста компании, а также информационную безопасность коммерческой организации, то можно выделить основные факторы, которые будут оказывать влияние и составлять угрозы на развитие компании:

1. Внешние факторы: экономические, природные, политические, социальные, технологические.

На экономические факторы могут оказывать значительное влияние конкуренция, спрос на товары или услуги, покупательская способность.

К угрозам природного характера относятся природные катаклизмы, стихийные бедствия, которые могут нанести серьёзный ущерб зданию, оборудованию, а также ограничить доступ к ресурсам компании. Законодательство, государственная политика, изменение налогообложения также могут повлиять на развитие компании. Например, за последние два года, с момента вступления в силу законов об ограничении мест и времени продажи алкоголя и табака, мелкий и средний бизнес понёс существенные потери. Демографическая ситуация, смена жизненных приоритетов населения и, как следствие, изменение спроса на продукты и услуги в разные промежутки времени влияют на экономическую составляющую бизнеса. В последние годы развитие новых технологий, распространение электронной коммерции ведут к переходу бизнеса от традиционных способов ведения торговли к торговле через Интернет. Параллельно с этим развиваются следующие виды угроз: внешние проникновения в систему; непреднамеренное (человеческий фактор) и преднамеренное изменение данных; преднамеренный перехват и чтение информации; взлом программно-аппаратной защиты; вирусные атаки и прочие угрозы электронной коммерции. Компания «InfoWatch» провела анализ, согласно которому на предприятиях и в компаниях информационная безопасность находится на низком уровне. По данным 2013 – 2014 гг., значительная доля потерь информации приходится на съёмные носители, электронную почту и сеть (рисунок 2) [4]. Однако все эти каналы легко перекрыть внутри самих компаний, тем самым значительно снизив вероятность потерь информации.

Рисунок 2 – Распределение по каналу утечки. Доли

Много говорится в СМИ и о том, что очень часто сами сотрудники компаний ошибочно либо осознанно «сливают» информацию. Об этом свидетельствуют следующие факты: в небольших и средних компаниях на долю сотрудников приходится 75,8 % утечек, в то время как в крупном бизнесе на долю сотрудников приходится лишь 44,8 % утечек (рисунок 3) [4].

Рисунок 3 – Распределение по виновнику утечки. Доли

2. Внутренние факторы: инфраструктурные, кадровые, операционные, технологические. Доступ к электронным ресурсам должен обеспечиваться бесперебойно и с минимальными задержками по времени. Это является основой для экономического роста компании. Поддерживать надёжность такого доступа должно своевременное техническое обслуживание электронного оборудования, обеспечивающего постоянный доступ к информационным ресурсам. Как следствие, количе-

ство простоев оборудования снижается, а лояльность клиентов повышается.

Квалификация сотрудников компании также играет немаловажную роль в электронном бизнесе. Ошибки на рабочем месте, мошенничество, шпионаж – всё это является причиной остановки бизнес-процессов. В том случае, если пропускная способность процессов снижается, то это может привести к неудовлетворённости покупателей продуктов или услуг, а также потере доли рынка.

Итак, обеспечение информационной безопасности бизнеса сводится к решению двух важных задач: обеспечение сохранности и целостности информации и защита информации от несанкционированного доступа. Основные выводы заключаются в том, что решать эти задачи лучше всего следующим образом:

1. За счёт использования облачных сервисов.

2. Путём ограничения и разграничения доступа. Необходимо минимизировать использование съёмных носителей. Каждый сотрудник должен работать в локальной сети только с той информацией, которая ему необходима для выполнения своих должностных обязанностей.

3. Создание архивов информации.

4. Постоянная поддержка антивирусной защиты.

5. Регулярное проведение планового технического обслуживания оборудования.

6. Обучение сотрудников работе с необходимым программным обеспечением. Проведение бесед по информационной безопасности на предприятии.

7. Применение шифрования информации, использование ЭЦП.

8. Проведение тщательного отбора и проверки сотрудников предприятия психологами, службой безопасности для исключения элементов шпионажа и «слива» информации.

Список использованных источников

1. Ясенев В. Н. Информационная безопасность в экономических системах : учеб. пособие / В. Н. Ясенев. Н. Новгород : Изд-во ННГУ, 2006.

2. Горохов П. К. Информационная безопасность / П. К. Горохов. М. : Радио и связь, 2005.

3. Степанов Е. А. Информационная безопасность и защита информации / Е. А. Степанов, И. К. Корнеев. М. : ИНФРА-М, 2008.

4. URL: http://www.infowatch.ru/ (дата обращения 05.03.2015).