**Татьяна СТАНИСЛАВЧУК,**
**Молдавская экономическая академия**

# ЭКОНОМИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

*In this report are considered the economic bases of information security and are proposed some rules for its creating. This work introduces the economic evaluation of a security framework and identifies the necessity and importance of security investment, in order to avoid cost and risks of a security breach.*

Любая система вне зависимости от того, государство это, компания или человек, стремится выжить, существовать и развиваться. Без обеспечения безопасности, как процесса, это невозможно. Таким образом, безопасность есть первая жизненная потребность любой системы и основная ее жизненная ценность.

Объектом защиты корпоративной системы безопасности являются ресурсы в самом широком смысле: информация, интеллектуальная собственность, активы, имущество, клиенты, персонал, технологии и так далее. Сама система управления компанией также является определенным ресурсом и требует защиты. Управление должно быть построено так, чтобы система безопасности не замыкалась в отдельной структуре. Обеспечение безопасности – это забота не только службы безопасности, но и всего менеджмента компании. Система должна охватывать всех сотрудников, начиная с президента компании и заканчивая техническим персоналом. Локализация управления безопасностью в одном департаменте может быть эффективна только в том случае, если бизнес устоялся и ничего не меняется. Когда же рынок динамично развивается, нужна гибкая система. Управление безопасностью – это развивающийся процесс.

Причины роста интереса к информационной безопасности (ИБ):

- глобализация распространения и проникновения информационных технологий (ИТ) во все виды человеческой деятельности;
- принципиальная зависимость ИТ от уровня ИБ;
- признание ИБ как значимого фактора экономического и политического развития (экономика – уровень бизнес-рисков).

Одна из аксиом безопасности гласит: безопасность – это проблема людей. Отсюда вывод: источником угроз являются люди. Система безопасности строится людьми и управляет людьми. Требования безопасности должны настолько войти в кровь и плоть сотрудников, чтобы они следовали им, не задумываясь. Такой подход может уберечь от серьезных проблем.

Так, основными целями защиты информации являются:

- предотвращение утечки, хищения, искажения, подделки информации в организации;
- предотвращение несанкционированных действий по уничтожению, искажению, блокированию информации;
- защита конституционных прав граждан (работников организации) на сохранение личной тайны и конфиденциальности персональных данных;
- сохранение коммерческой тайны, конфиденциальности документированной информации.

Мероприятия по обеспечению информационной безопасности (ИБ), как известно, не приносят доходов, с их помощью можно лишь уменьшить ущерб от возможных инцидентов. Поэтому очень важно, чтобы затраты на создание и поддержание ИБ на должном уровне были соразмерны ценности активов организации, связанных с ее информационной системой (ИС).

Нарушения безопасности коммерческих организаций приводят к финансовым потерям, связанным с выходом из строя сетевого оборудования при ведении электронной коммерции. Кроме того, с оплатой сверхурочной работы ИТ-персонала и/или оплатой работ подрядчиков, занимавшихся восстановлением корпоративной информационной системы. В эту же статью расходов следует включить затраты на консультации внешних специалистов, восстановление данных, ремонт и юридическую помощь, судебные издержки при подаче искового заявления о виртуальных преступлениях и нарушениях политики безопасности. Вместе с тем необходимо помнить и о нанесении ущерба имиджу и репутации компании.

С целью «смягчить» ожидаемые потери, компании необходимо инвестировать средства в инструменты обеспечения безопасности. Стоимость системы информационной безопасности складывается из единовременных (покупка лицензий антивирусного программного обеспечения, инструментария Firewall, приобретение аппаратных средств, а также на оплату консультаций внешнего эксперта в области информационной безопасности) и периодических затрат (стоимость

технической поддержки и сопровождения, расходы на заработную плату ИТ-персонала, на найм необходимых специалистов, а также на исследование угроз нарушений политики безопасности).

Обоснование расходов на информационную безопасность, как правило, включает в себя следующие утверждения:

- расходы на безопасность являются составляющей стоимости ведения бизнеса;
- расходы на безопасность родственны расходам на страхование;
- компания не может заниматься электронной коммерцией без обеспечения определенного уровня защиты электронных денежных потоков;
- безопасность - один из аспектов управления рисками;
- заказчик имеет право подать на компанию в суд, если она отказывается соблюдать минимальные стандарты безопасности (например, защищать конфиденциальную информацию о клиенте);
- нежелание вкладывать денежные средства в безопасность означает нежелание следовать общим тенденциям развития информационных технологий.

*При построении ИБ следует придерживаться следующих правил:*

1. Существуют три понятия: безопасность, скорость и дешевизна, просто невозможно выбрать только два из них.
2. В управлении безопасностью, как отрасли производства, действуют все экономические законы и понятия, например эффективность, хотя рассчитать ее несколько сложнее, чем обычную эффективность, так как здесь эффектом является не прибыль, а экономия.
3. Безопасность и сложность – явления обратно пропорциональные. Чем сложнее процесс, тем больше проблем с безопасностью, тем менее он надежен. Чем сложнее вопросы, тем более дорогостоящая система требуется.
4. При отсутствии прочих факторов всегда используйте вариант с наибольшей безопасностью.
5. Безопасность – инвестиция, а не расход. Стоит она дорого, что оправданно, но это совсем не значит, что в нее можно вкладывать бесконечно.
6. Любая система безопасности тормозит развитие системы в целом. Единственный выход – следовать за изменениями, меняться вслед за бизнесом, прогнозировать неведомое. Наиболее эффективно управление безопасностью там, где оно непосредственно включено в бизнес-процессы.

Внедрение или модернизация информационной системы приводит, как правило, к значительному повышению эффективности бизнеса, а также его конкурентоспособности. Но случается и обратное: предприятие терпит реальные убытки от внедренной информационной системы, если в ней не предусмотрены адекватные средства защиты информации, поэтому оценка её после внедрения обязательна.

Обеспечение информационной безопасности – сложный, многоаспектный процесс, требующий принятия множества решений, анализа множества факторов и требований. Базой для системного подхода к обеспечению ИБ могут служить минимальные требования безопасности:

- политика ИБ;
- оценка рисков;
- планирование;
- сертификация, аккредитация и оценки ИБ;
- протоколирование и аудит;
- обеспечение целостности;
- аутентификация и авторизация;
- физическая защита;
- управление конфигурацией;
- действия ИБ к сервисам и системам;
- защита систем и телекоммуникаций;
- защита носителей;
- мониторинг регуляторов ИБ;
- информирование и обучение персонала;
- кадровая безопасность;
- реагирование на нарушение ИБ.

Анализируя всё вышеперечисленное, может быть предложено следующее:

- Следует использовать ту возможность, которую предлагают нормативные акты – сделать ИТ-

безопасность интегрированной частью бизнес-процессов. А именно: увеличить инвестиции в обеспечение совместимости с нормативными актами с целью улучшить ключевые элементы функций ИТ-безопасности: архитектуру и организационную структуру; объединить процессы обеспечения совместимости с процессами ИТ-безопасности, чтобы повысить эффективность первых и комплексно покрыть риски; установить баланс между усилиями по реализации корпоративных политик и процедур и усилиями по достижению деловых целей организации.

- Сделать сотрудничество с третьими фирмами более эффективным, особенно в области совместной работы и аутсорсинга. А именно: принять формальные процедуры, включая систему оценки рисков, чтобы корректно учитывать риски компаний-партнеров; требовать независимого аудита или сертификации в компаниях-партнерах, чтобы минимизировать новые риски и воспользоваться всеми плодами аутсорсинга; принять признанные стандарты ИТ-безопасности для своей собственной компании, чтобы продемонстрировать клиентам и заказчикам высокий уровень безопасности на своем предприятии.
- Принять ряд мер, чтобы сделать использование новых технологий более безопасным. А именно: адекватно оценить риски, которым подвергается организация ввиду использования новых технологий, особенно те, которые связаны с недостаточным внутренним контролем или целиком зависят от поведения пользователей; принять комплексные меры минимизации рисков: проводить тренинги и обучать персонал, донести до каждого его ответственность в плане безопасности.
- Сделать все возможное, чтобы ИТ-безопасность ориентировалась на стратегические цели организации. А именно: объединить ИТ-безопасность с всесторонним процессом управления рисками в компании; регулярно встречаться с директорами коммерческих отделов и советом директоров, чтобы объяснить высшим исполнительным лицам, как ИТ-безопасность может помочь им в реализации их собственных проектов, и отчитаться по проектам и инцидентам ИТ-безопасности, а также по процессам обеспечения совместимости; перераспределить ресурсы и бюджет на те задачи, которые отвечают стратегическим целям организации – автоматизировать рутинные операции и передать специализированные процессы, например, реакцию на инциденты и управление проектами, на аутсорсинг; пройти процесс сертификации или принять стандарт, который предоставляет достаточную базу, чтобы внедрить эффективные положения ИТ-безопасности, отвечающие стратегическим целям организации.

Эффективная работа современной службы безопасности невозможна без понимания и доверия на всех уровнях управления компанией.

Рынок Молдовы достаточно молод. Ресурсов мало, субъектов много. Постоянно идет конкурентная борьба за эти ресурсы и преимущества на рынке. В инвестиционном и финансовом бизнесе службам безопасности приходится проверять практически всех своих контрагентов и клиентов, изучать конкурентов, анализировать потоки информации, заниматься моделированием и прогнозом ситуаций. Это дает возможность избежать как финансовых, так и, самое главное, имиджевых потерь. Информация и анализ сегодня решают все.

**Литература:**


1. Holbein R, Gaugler T. IT security electronic commerce: from cost to value. DEXA Workshop; 1999
2. Anderson R. Why information security is hard (An Economic Perspective). In: 17th Annual computer security applications conference; December 2001
3. Батурин Ю.М., Жиджитский А.М. Компьютерная преступность и компьютерная безопасность. - М.: Юридическая литература, 1991
4. Осипов А. Как рассчитать стоимость ИТ-услуги. - Журнал: КомпьютерПресс, Сентябрь 2007.