АНАЛИЗ ПЕРЕДОВЫХ ПОДХОДОВ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Смоквина А.А., к.э.н., доцент
Велиева М.А.

Одесский национальный политехнический университет, г. Одесса

В условиях современной нестабильности рыночных отношений успех организации стал тесно взаимосвязан с его способностью управлять рисками особенно что касается микроуровня, то есть уровень субъектов хозяйствования. Поскольку компании становятся все более зависимыми от информации, способность защищать важную и секретную информацию стало стратегически необходимым для обеспечения устойчивости предприятия, рентабельности и общей стоимости предприятия.

К сожалению, руководство предприятий не всегда рассматривает информационную безопасность в качестве стратегического приоритета в области защиты и как средство для содействия достижению стратегических целей организации. В то время как обеспечение информационной безопасности становится необходимым условием для устойчивого прогресса организации, по следующим причинам: поддержание конкурентного преимущества, защита репутации, обеспечение соблюдение законов и правил.

Основные факторы, влияющие на информационную безопасность предприятия:

- расширение сотрудничества предприятия с партнерами;
- автоматизация бизнес-процессов на предприятии;
- расширение кооперации исполнителей при построении и развитии информационной инфраструктуры предприятия;
- рост объемов информации предприятия, передаваемой по открытым каналам связи;
- рост компьютерных преступлений [1].

Система обеспечения информационной безопасности представляет собой совокупность мер, которые можно условно разделить на организационный уровень и программно-технический уровень, направленные в свою очередь на защиту информационных ресурсов предприятия от угроз информационной безопасности [2]. Структура обеспечения информационной безопасности представлена на рис.

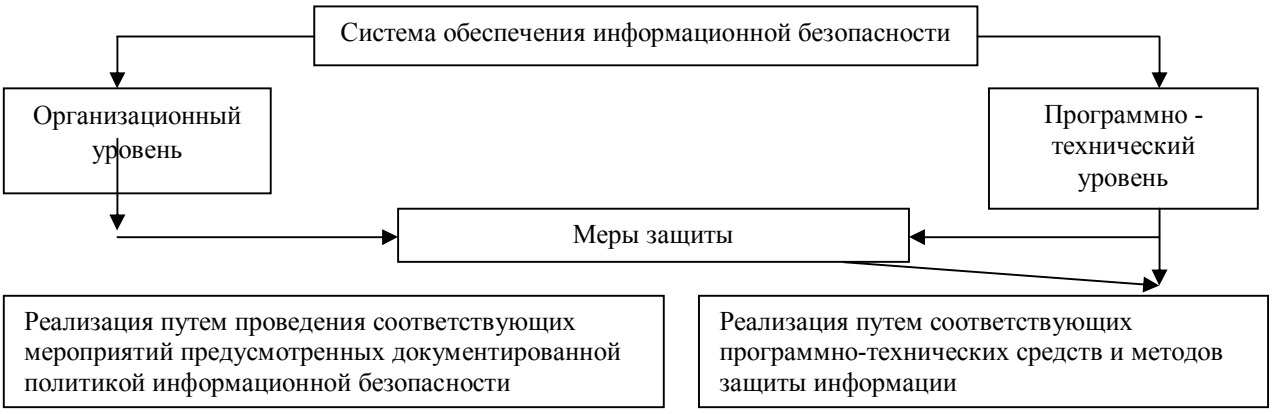

Рис. 1. Структура обеспечения информационной безопасности

Возможность реализации угроз зависит от наличия уязвимых мест, состав которых определяется видом решаемых задач, характером обрабатываемой информации, аппаратно-программными особенностями обработки информации на предприятии, наличием средств защиты и их характеристиками. Выделяют несколько основных групп угроз информационной безопасности:

– Непреднамеренные (случайные) угрозы - выражаются в неадекватной поддержке механизмов защиты и ошибками в управлении.

– Преднамеренные угрозы - выражаются в несанкционированном получение информации и несанкционированной манипуляции данными, ресурсами и самими системами.

Сегодня главной угрозой информационной безопасности для Украинских предприятий являются мобильные накопители примерно 70%, электронная почта 50-55%, Интернет форумы 30-35%

Что касается организации и проведения работ по обеспечению информационной безопасности предприятия, то они определяются действующими государственными и международными стандартами и другими нормативными и методическими документами.

В мировой практике существует много подходов для непрерывного совершенствования информационной безопасности, среди которых следует выделить ISO / IEC 27001: 2013 (ISO 2013). Эта модель определяет требования к созданию, внедрению, поддержанию и постоянного совершенствования системы управления информационной безопасностью в контексте организации. Она также включает в себя требования к оценке и обработки рисков информационной безопасности с учетом потребностей организации. Требования, изложенные в ISO / IEC 27001: 2013 являются общими и предназначены для применения ко всем организациям, независимо от типа, размера или характера. Однако этот подход имеет существенный недостаток: аудит ориентирован в основном на политическую и передовую практики и тем самым упускает возможности для активного совершенствования, направленного на достижение состояния совершенства безопасности.

Модель EFQM представляет собой структуру управления, которая позволяет организациям всех типов и размеров, оценить их прогресс на пути к совершенству бизнеса, помогая им определить ключевые сильные стороны и недостатки в отношении практики их видения и миссии. В ряде организаций, эта модель используется для интеграции инструментов и методов управления в целостной структуре, направленной на поддержку целей организаций.

Модель EFQM объединяет три компонента:

1) Фундаментальные понятия совершенства набор основополагающих принципов, на основе ряда европейских ценностей, происходящих в Европейской конвенции о защите прав человека и Европейская социальная хартия, закладывает необходимый фундамент для достижения устойчивого превосходства в любой организации ((EFQM, 2012)

2) Модель является сама по себе опорным каркасом структурированная по критериям, которые могут быть использованы для оценки и направлять инициативы организации и результаты к совершенству.

3) RADAR логика или непрерывное совершенствование предлагает структурированный подход к рассмотрению организационной эффективности, но и закладывает основу систематического непрерывного процесса совершенствования.

С целью обеспечения конфиденциальности и целостности передаваемых или сохраняемых данных международная организация по стандартизации (ИСО) и международный электротехнический комитет (МЭК) совместно разработали новый стандарт, определяющий механизмы шифрования ID пользователя, которые позволят обеспечить оптимальный уровень защиты.

С учетом развития электронных сделок, предполагающих передачу личной, коммерческой или банковской информации, новый стандарт ИСО/МЭК соответствует возрастающей потребности в выполнении требований к безопасности информации, которая обеспечивает:

– Конфиденциальность данных (защита от несанкционированного использования);

– Целостность данных (позволяет пользователю защитить свои данные от изменения другими пользователями);

– Подтверждение подлинности данных.

Новый стандарт учитывает специфические потребности в безопасности, присущие различным операциям. Так, например, применение цифровой подписи, является идеальным способом защиты данных от изменения другими лицами. Некоторые ситуации могут потребовать сочетания ряда операций, но не все комбинации гарантируют адекватную защиту.

Механизмы, определяемые новым стандартом были разработаны с целью максимального повышения уровня безопасности и обеспечения эффективной обработки данных. Также стандарт включает специфичные механизмы, которые могут применяться для обеспечения целостности данных даже без их шифрования (например, для предотвращения изменения адресов электронной почты и порядковых номеров данных).

Таким образом, в каждом конкретном случае при выборе подхода к обеспечению информационной безопасности необходимо выбрать такую модель или комбинацию моделей, которая принимала бы во внимание как можно больше результирующих факторов, присущих данной системе, и наиболее достоверно определяла вероятность реализации наихудшего сценария. При этом такая модель должна динамично изменять исходные результаты при изменении масштаба и качества субъектов и объектов системы, например: количество пользователей, количество комутации оборудования, скорость канала передачи данных.

Література

1. Преображенский Е. Инсайдерские угрозы в России`09 // Управление персоналом // Корпоративная Периодика. -2009. - №7(209). - С. 6-10.
2. Крошилин С.В., Медведева Е.И. Информационные технологии и системы в экономике: учебное пособие. - М.: ИПКИР, 2008. - 485с.
3. Системний підхід до інформаційного забезпечення внутрішнього контролю [Електронний ресурс] / В.Ф. Максімова., Н.М. Албу // Економіка: реалії часу. Науковий журнал. – 2014. – № 4 (14). – С. 73-77. – Режим доступу до журн.: http://economics.opu.ua/files/archive/2014/n4.html.
4. Система формування і забезпечення економічної безпеки підприємства [Електронний ресурс] / С.В. Філиппова, О.С. Дашковський // Економіка: реалії часу. Науковий журнал. – 2012. – № 2 (3). – С. 17-21. – Режим доступу до журн.: http://www.economics.opu.ua/n3.html.
5. Концептуальні засади управління економічно-безпечним інноваційним розвитком промислового підприємства та формування його аналітичних інструментів [Електронний ресурс] / Л.О. Волощук // Економіка: реалії часу. Науковий журнал. – 2015. – № 1 (17). – С. 234-241. – Режим доступу до журн.: http://economics.opu.ua/files/archive/2015/n1.html
6. Філиппова С.В. Економічна безпека підприємств реального сектору економіки в умовах вартісно-орієнтованого управління: монографія / С. В. Філиппова, Л. О. Волощук, С. О. Черкасова / під заг. ред. С. В Філиппової. – Одеса: ФОП Бондаренко М.О., 2015. – 196 с.