**ТЕХНОЛОГИЯ ЗАЩИТЫ ДАННЫХ В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ**

**DATA PROTECTION TECHNOLOGY IN CORPORATE INFORMATION SYSTEMS**

Сень З.В. и Закревский Н. А.

Санкт-Петербургский государственный экономический университет,

г. Санкт-Петербург, Россия

В данной работе рассмотрены концепции корпоративных информационных систем. Подробно изучена система планирования ресурсов предприятия Enterprise Resource Planning System, на основе которой разобраны существующие угрозы корпоративных информационных систем и проанализированы методы их минимизации или полного устранения.

Ключевые слова: корпоративные информационные системы, информационные технологии, информационная безопасность, меры защиты, концепция.

This research paper discusses the concepts of corporate information systems. The Enterprise Resource Planning System has been studied in detail, which is used to analyze existing threats to corporate information systems and analyze methods for minimizing or completely eliminating them.

Keywords: corporate information systems, information technologies, information security, security measures, concept.

Корпоративные информационные системы (КИС) стали неотъемлемой частью любой компании. Они позволяют существенно повысить внутреннюю управляемость организацией. Следствием этого становится увеличение объемов продаж, снижение себестоимости, оптимизация складских запасов, сокращение сроков выполнения заказов, повышение качества взаимодействия с контрагентами и, в конечном счете, повышение прибыли.

В связи с тем, что в корпоративных информационных системах хранится ценная информация, нарушение целостности или конфиденциальности которой может привести к краху целого предприятия остро стоит вопрос о защите информации в корпоративных информационных системах.

Для начала обратимся к концепция объемно-календарного планирования MPS (Master Planning Schedule). Данная концепция является основой всех корпоративных информационных систем, основной задачей которых является планирование. Применяется главным образом на производственных предприятиях.

Следом идет концепция MRP (Material Requirements Planning) – концепция планирования потребности в материальных ресурсах. Ее основной задачей является определение потребности в ресурсах на основе результатов объемно-календарного планирования и подробных спецификаций состава производимой продукции.

Далее CRP (Capacity Requirements Planning) – концепция планирования производственных мощностей. В этой концепции основой является спецификация технологических операций, необходимых при производстве изделия.

FRP (Finance Requirements Planning) – концепция планирования финансовых ресурсов.

MRPII (Manufacturing Resources Planning) – концепция планирования ресурсов производства. Включает MRP, CRP и FRP во взаимосвязи.

Чтобы осуществить грамотное планирование ресурсов, синхронизированное с клиентом, используется CSRP (Customer Synchronized Resources Planning). Эта концепция включает в себя всю цепь от проектирования будущего продукта на основе требований заказчика до продажи и последующего сервисного обслуживания.

SCM (Supply Chain Management) – концепция управления цепочками поставок. SCM-системы ориентированы на оптимизацию логистических цепей. Как правило, является составной частью ERP и MRPII-систем.

Остановимся поподробнее на системе планирования ресурсов предприятия Enterprise Resource Planning System. Данная корпоративная информационная система, предназначена для автоматизации учета и управления.

Системы данного вида строятся по модульному принципу и охватывают все ключевые процессы деятельности компании. Используемый в ERP-системах программный инструментарий позволяет проводить производственное планирование, моделировать поток заказов и оценивать возможность их реализации в службах и подразделениях предприятия.

Основные функции ERP - систем:

* ведение конструкторских и технологических спецификаций, определяющих состав производимых изделий, а также материальные ресурсы и операции, необходимые для их изготовления;
* формирование планов продаж и производства;
* планирование потребностей в материалах и комплектующих, сроков и объемов поставок для выполнения плана производства продукции;
* управление запасами и закупками: ведение договоров, реализация централизованных закупок, обеспечение учета и оптимизации складских и цеховых запасов;
* планирование производственных мощностей от укрупненного планирования до использования отдельных станков и оборудования;
* оперативное управление финансами, включая составление финансового плана и осуществление контроля его исполнения, финансовый и управленческий учет;
* управление проектами, включая планирование этапов и ресурсов.

Корпоративная информационная система, как и любая другая информационная система подвержена угрозам безопасности.

Выделяют три основных типа угроз безопасности:

* нарушение конфиденциальности информации в корпоративных информационных системах. Угрозы нарушения конфиденциальности направлены на раз­глашение конфиденциальной или секретной информации. При реализации этих угроз информация становится известной лицам, которые не должны иметь к ней доступ;
* нарушение целостности информации в корпоративных информационных системах. Угрозы нарушения целостности информации, хранящейся в компьютерной системе или передаваемой по каналу связи, на­правлены на ее изменение или искажение, приводящее к наруше­нию ее качества или полному уничтожению;
* отказ в обслуживании корпоративных информационных систем. Угрозы нарушения работоспособности направлены на создание таких ситуаций, когда определенные пред­намеренные действия либо снижают работоспособность корпоративных информационных систем, либо блокируют доступ к некоторым ее ресурсам.

Угрозы могут быть классифицированы по нескольким параметрам:

* по величине принесенного ущерба:
  + предельный, после которого фирма может стать банкротом;
  + значительный, но не приводящий к банкротству;
  + незначительный, который фирма за какое-то время может компенсировать.
* по вероятности возникновения:
  + весьма вероятная угроза;
  + вероятная угроза;
  + маловероятная угроза.
* по причинам появления:
  + стихийные бедствия;
  + преднамеренные действия.
* по характеру воздействия:
  + активные;
  + пассивные.
* по отношению к объекту:
  + внутренние;
  + внешние.

Меры безопасности корпоративных информационных систем можно рассматривать как последовательность барьеров или рубежей защиты информации. Рассмотрим их подробнее.

Первый рубеж – правовой. Этот аспект защиты информации связан с необходимостью соблюдения юридических норм при передаче и обработке информации. К правовым мерамзащиты информации относятся действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией ограниченного использования и ответственности за их нарушения. Этим они препятствуют несанкционированному использованию информации и являются сдерживающим фактором для потенциальных нарушителей.

Второй рубеж защиты образуют морально-этические меры*.*К морально-этическим мерам противодействия относятся всевозможные нормы поведения, которые традиционно сложились или складываются в обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные, но их несоблюдение обычно ведет к падению престижа человека, группы лиц или организации.

Третьим рубежом, препятствующим неправомочному использованию информации, являются административные меры. Администраторы всех рангов с учетом правовых норм и социальных аспектов определяют административные меры защиты информации.

Административные мерызащиты относятся к мерам организационного характера. Они регламентируют:

* процессы функционирования КИС;
* использование ресурсов КИС;
* деятельность ее персонала;
* порядок взаимодействия пользователей с системой, с тем чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности.

Административные меры включают:

* разработку правил обработки информации в КИС;
* совокупность действий при проектировании и оборудовании вычислительных центров и других объектов КИС;
* совокупность действий при подборе и подготовке персонала;
* организацию надежного пропускного режима;
* организацию учета, хранения, использования и уничтожения документов и носителей с конфиденциальной информацией;
* распределение реквизитов разграничения доступа;
* организацию скрытого контроля над работой пользователей и персонала КИС;
* совокупность действий при проектировании, разработке, ремонте и модификации оборудования и программного обеспечения.

Важно отметить, что, пока не будут реализованы действенные меры административной защиты, прочие меры будут, несомненно, неэффективны.

Четвертым рубежом являются физические меры защиты*.*К физическим мерам защиты относятся разного рода механические, электро- и электронно-механические устройства или сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации.

Последним рубежом являются аппаратно-программные средства защиты*.*К ним относятся различные электронные устройства и специальные программы, которые реализуют самостоятельно или в комплексе с другими средствами следующие способы защиты:

* идентификацию и аутентификацию субъектов КИС;
* разграничение доступа к ресурсам КИС;
* контроль целостности данных;
* обеспечение конфиденциальности данных;
* регистрацию и анализ событий, происходящих в КИС;
* резервирование ресурсов и компонентов КИС.

Таким образом, становится понятным, что одним из главных шагов на пути к обеспечению конфиденциальности информации является разграничение доступа сотрудников к ресурсам корпоративной информационной системы с целью ограничить спектр информации необходимой тому или иному сотруднику.

Подводя итоги, можно сказать, что построение комплексной системы корпоративной безопасности оказывается настолько сложной задачей, насколько сложны технологические процессы компании. Грамотный и своевременно составленный план защиты способен снизить степень большинства рисков. Однако, перечисленные методы не исчерпывают весь спектр возможных решений, тем не менее их применение будет способствовать эффективному использованию существующих и перспективных корпоративных информационных систем, что позволит изменить жизнь человека как потребителя услуг, предоставляемых информационными технологиями.

**СПИСОК ЛИТЕРАТУРЫ:**

1. Девянин, П.Н., Михальский, О.О., Правиков, Д.И., Щербаков, А.Ю. Теоретические основы компьютерной безопасности. [Текст] / П.Н. Девянин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербаков. - М.: Радио и связь, 2000.

2. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. [Текст] / А.А. Малюк. - М.: Горячая Линия-Телеком, 2004.

3. Информационный портал «Википедия» [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org (дата обращения: 06.04.20).