УДК 338

РАЗВИТИЕ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

© 2011 А.В. Казакова*

Ключевые слова: информационная безопасность, защита информации, система информационной безопасности, информационные угрозы, информационная система, конфиденциальная информация

Представлены основные причины неэффективности организационного построения информационных систем. Рассматриваются возможности для формирования системы обеспечения информационной безопасности на промышленных предприятиях Самарской области. Определены классы информационных ресурсов. Характеризуются современные методы оценки затрат и способы обоснования инвестиций в информационную безопасность промышленных предприятий. Раскрывается сущность политики информационной безопасности.

Развитие промышленных предприятий России показывает, что руководство уже принимает некоторые меры по защите важной информации, однако эти действия не носят системного характера, поскольку направлены на устранение отдельных угроз, оставляющих за собой множество уязвимых мест[1]. Также одной из основных причин проблем промышленных предприятий в сфере обеспечения информационной безопасности является отсутствие продуманной и утвержденной политики в этой области, базирующейся на организационных, экономических и технических решениях с последующим контролем их реализации и оценкой эффективности. Обострение проблем информационной безопасности в условиях интенсивного совершенствования технологий и инструментов защиты данных является следствием роста и усиливающейся тяжести их последствий. Все это определяет необходимость разработки системы обеспечения информационной безопасности промышленных предприятий.

Оценку организации информационных процессов на промышленных предприятиях Самарской области целесообразно проводить посредством анализа структуры и функций информационных систем управления. Существующие информационные системы машиностроительных предприятий условно можно подразделить на две категории: информационные системы, организованные по принципу централизованной обработки информации; информационные системы, организованные по принципу централизованной обработки информации с использованием элементов децентрализации.

Анализ существующих систем обработки информации, в большей степени определяющих использование информационного ресурса позволил выявить недостатки организационного характера, сдерживающие процессы максимального использования информационного потенциала производства.

К основным причинам неэффективности организационного построения информационных систем можно отнести следующие:

- отсутствие разработанных организационных принципов взаимодействия субъектов хозяйствования в регионе; отсутствие системного подхода к проблеме информатизации управленческой деятельности, информационной согласованности решаемых управленческих задач как внутри функциональных подразделений, так и с задачами других подсистем. В итоге - снижение оперативности, достоверности и качества результативной информации;
- статичную структуру решаемых информационной системой задач с применением жесткого алгоритма и периодичности решения, как следствие - отсутствие способности реагирования на возмущающие воздействия (изменения информационной базы, структуры выходных функций и т. д.), привлечение больших дополнительных трудозатрат для обеспечения должного уровня оперативности, достоверности и полноты информации;

* Казакова Арина Валерьевна, аспирант Самарского государственного экономического университета. E-mail: arina-21@mail.ru.

♦ значительное запаздывание информационных потоков относительно материальных. По оценке специалистов, запаздывание отдельных видов информации достигает 30 дней. Результат - снижение ценности информационного продукта и возможности его дальнейшего использования; отрыв информации от первоисточника, в результате - низкая достоверность получаемой информации (40-45 %).

Кроме того, на исследуемом предприятии применяется централизованная форма обработки информации, вследствие чего обнаруживается слабое знание пользователями специфики и возможностей средств вычислительной техники в подготовке управленческих решений, негативное отношение к применению информационных технологий в управленческой деятельности.

Инертность существующих информационных систем, низкое качество предоставляемой информации, "пакетный" режим обработки, незначительная диалоговая поддержка не обеспечивают эффективности использования информационных ресурсов. Повышение уровня эффективности видится в создании информационно совместимых технологий на предприятии, начиная с каждого рабочего места. Скажем, в своих ежегодных отчетах по деятельности ОАО "ВБМ" указывает следующие. В течение 2008 г. были введены в эксплуатацию 19 новых компьютеров в подразделениях предприятия, в 2009 г. этот показатель составил 22 единицы. Были проведены работы по дальнейшему развитию локальной сети предприятия. Проводилась работа по развитию информационной системы предприятия: завершается 4 этап разработки информационной базы данных "Техническая подготовка долотного производства "SmarTeam". Тестирование разработок по 4 этапу предполагается завершить в феврале 2009 г.; разработана программа складского учета дорогостоящих материалов (сталь, твердосплавные материалы, бронзы) на складах ОМТС.

Вышеупомянутые тенденции являются единственным упоминанием в отчетных документах общества, касающиеся информатизации промышленного предприятия. Несколько иная картина связана деятельностью ОАО "Кузнецов". Подробный анализ деятельности ОАО "Кузнецов" позволяет сделать вывод, что в связи с реализацией программы развития в настоящее время будет уделяться серьезное внимание проблеме информатизации и автоматизации деятельности, а следовательно, как никогда остро встанет вопрос об обеспечении информационной безопасности. Исследуемые предприятия не имеют достаточных возможностей для формирования системы обеспечения информационной безопасности, поэтому целесообразно активизировать информационные функции как в системе формирования, так и в системе использования информационных ресурсов и в системе обеспечения безопасности.

Информационная безопасность служит функциональным элементом системы обеспечения стратегического развития промышленного предприятия, поэтому ее основная задача - обеспечить стабильность существования предприятия в настоящем и перспективы его устойчивого развития в будущем. Основной предпосылкой к созданию системы защиты информации является ее значимость как инструмента и ресурса бизнеса и угроза для предприятия понести материальный ущерб от утечки информации. На основе данных критериев систему информации промышленного предприятия можно отнести к различным классам по степени важности и необходимости обеспечения их защиты (табл. 1).

Документация - необходимое условие гарантированной надежности системы и, одновременно, - инструмент проведения политики безопасности. Без документации люди не будут знать, какой политике следовать и что для этого нужно делать. В комплект документации надежной системы должны входить следующие тома: руководство пользователя по средствам безопасности; руководство администратора по средствам безопасности; тестовая документация; описание архитектуры. Разумеется, на практике требуется еще по крайней мере одна книга - письменное изложение политики безопасности организации. Руководство пользователя по средствам безопасности предназначено для обычных, непривилегированных людей. Оно должно содержать сведения о механизмах безопасности и способах их использования.

"Критерии" Министерства обороны США открыли путь к ранжированию информационных систем по степени надежности. Заим-

Таблица 1

Классы информационных ресурсов организации

Класс	Содержание
5-й "открытая информация"	Общие сведения о предприятии и характере его деятельности, необходимые для составления публикуемых годовых отчетов, пресс-релизов, публикаций о предприятии в СМИ, рекламной и агитационной продукции
4-й "служебная информация"	Сведения, широко применяемые в повседневной работе предприятия и опубликование которых вне организации или нарушение их целостности причинило бы предприятию беспокойство, не нанеся при этом значимых материальных потерь или серьезного ущерба имиджу предприятия. Примером подобной информации могут быть служебные записки, расписание встреч, текущие данные, правила внутреннего распорядка и т.п.
3-й "конфиденциальная информация"	Сведения о контрагентах предприятия и условиях работы с ними, о процедурах, методике и формах управления предприятием, разработанных или освоенных на предприятии, находящиеся на начальной стадии бизнес-проекты организации, а также документы, определяющие общие планы и перспективы развития предприятия, потенциально способные обеспечить конкурентное преимущество организации в будущем
2-й "строго конфиденциальная информация"	Сведения, содержащие аналитическую обработку результатов бухгалтерского учета, производственной, маркетинговой, управленческой деятельности организации, деловые планы и бизнес-проекты, предопределяющие конкретные направления развития предприятия и сферы приложения его усилий с целью укрепления и развития собственного конкурентного преимущества, собственные перспективные дизайнерские разработки, описание информационной политики предприятия, структура и методы работы системы экономической безопасности организации, в том числе и по информационной составляющей, информация о конкурентах, собранная методами бизнес-разведки
1-й "абсолютно конфиденциальная информация"	Важные внутренние документы организации, в том числе инвестиционные, маркетинговые, производственные и управленческие стратегии и стратегические приоритеты предприятия, программы поглощения и слияния компании и другая информация, разглашение или разрушение которой способно нанести фатальный ущерб организации

ствуем и адаптируем данную методику. Определяется четыре уровня безопасности (надежности) - D, C, B и A. Уровень D предназначен для систем, признанных неудовлетворительными. В настоящее время он содержит две подсистемы управления доступом для ПК. По мере перехода от уровня C к A к надежности систем предъявляются все более жесткие требования. Уровни C и B подразделяются на классы (C1, C2, B1, B2, B3) с постепенным возрастанием надежности. Таким образом, всего имеется шесть классов безопасности - C1, C2, B1, B2, B3, A1. D1 - неудовлетворительная безопасность; C1, C2 - произвольное управление доступом; B1, B2, B3 - принудительное управление доступом; A1 - верифицированная защита.

Для построения комплексной системы информационной безопасности предприятия необходимо определить характер процессов, происходящих в информационной системе организации, и специфику возникновения и реализации угроз, а также систему мер и методов для защиты информации различных классов. Поэтому следует проследить процесс возникновения и реализации угроз: очевидно, что существующий источник негативного воздействия, активизируясь, генерирует угрозу, которая для предприятия реализуется в атаке на информационную систему организации (информационном инциденте), затем атака воздействует на уязвимость организации, что и приводит к возникновению ущерба. В идеале комплексная система защиты собственных информационных ресурсов должна охватывать все стадии данного процесса, что позволит обеспечить максимальную защищенность информационной системы предприятия, не допустить наступления ущерба или свести его проявление к минимуму. Таким образом, в основу построения любой системы собственной информационной безопасности должна быть положена оборонительная стратегия, которая включает в себя комплекс мер защитного характера.

Для защиты информационных ресурсов необходимо введение контролирующих процедур. Их задача мониторинг информационной системы организации с целью распознания возникающих информационных инцидентов и анализ уязвимостей информационной среды, что позволяет инициировать защитные мероприятия не по факту негативного воздействия на уязвимость или возникновению ущерба, а с момента начала информационной атаки.

Внедрение в систему информационной безопасности предприятия контролирующих мероприятий позволяет организации перейти к реализации наступательной стратегии, обеспечивающей защиту информационных ресурсов организации по всему спектру уязвимостей от большинства атак, но существует реальная угроза возникновения частичного ущерба вследствие возникновения нового источника угроз и его негативного воздействия на информационную систему организации, что экономически недопустимо для строго конфиденциальной или абсолютно конфиденциальной информации, поскольку даже частичное нарушение их свойств способно вызвать значительные финансовые потери или дискредитацию организации в целом в глазах контрагентов или государственных структур.

Методика построения системы безопасности собственных информационных ресурсов, опирающаяся на оценку рисков информационной безопасности организации, разделения информационных ресурсов внутрифирменного обращения на классы по степени важности для осуществления основных видов деятельности предприятия и уязвимости для негативного воздействия и определение конкретных направлений защиты информации в зависимости от характерных особенностей ее создания, обработки, хранения и перераспределения, позволяет создать на конкретном предприятии максимально гибкую и адекватную условиям функционирования систему защиты, которая способна обеспечить оптимальный уровень информационной безопасности при рациональном использовании материальны и кадровых ресурсов организации.

С повышенными требованиями в области информационной безопасности затраты на обеспечение режима информационной безопасности составляют до 30 % всех затрат на информационную систему, и владельцы информационных ресурсов серьезно рассматривают экономические аспекты обеспечения информационной безопасности. Даже в тех информационных системах, уровень информационной безопасности которых явно недостаточен, у технических специалистов зачастую возникают проблемы обоснования перед руководством затрат на повышение этого уровня (табл. 2).

При проведении работ по созданию или модернизации системы информационной безопасности промышленного предприятия часто обращаются за помощью к внешним консультантам.

В вопросе передачи обеспечения безопасности информации на аутсорсинг многое зависит от решения руководства промышленного предприятия: готово ли оно идти на увеличение рисков, оправдано ли это экономически. По мнению некоторых экспертов в

Таблица 2

Современные методы оценки затрат и способы обоснования инвестиций в информационную безопасность промышленных предприятий

Методы оценки затрат на информационную безопасность	Способы обоснования инвестиций в информационную безопасность
Прикладной информационный анализ (Applied Information Economics) Потребительский индекс (Customer Index) Добавленная экономическая стоимость (Economic Value Added) Исходная экономическая стоимость (Economic Value Sourced) Управление портфелем активов (Portfolio Management) Оценка действительных возможностей (Real Option Valuation) Метод жизненного цикла искусственных систем (System Life Cycle Analysis) Система сбалансированных показателей (Balanced Scorecard) Совокупная стоимость владения (Total Cost of Ownership) Функционально-стоимостной анализ (Activity Based Costing)	Метод ожидаемых потерь - Метод оценки свойств системы безопасности (Security Attribute Evaluation Method) Анализ дерева ошибок (Fault Tree Analysis)

области информационной безопасности, в данном вопросе “должен быть достигнут разумный компромисс”.

Политика информационной безопасности является планом высокого уровня, в котором описываются цели и задачи мероприятий в сфере безопасности. Это ни директива, ни норматив, ни инструкция, ни средство управления. Политика описывает безопасность в обобщенных терминах без специфических деталей. Она обеспечивает планирование всей программы безопасности так же, как спецификация определяет номенклатуру выпускаемой продукции.

Под политикой информационной безопасности понимается совокупность документированных управленческих решений, направленных на защиту информационных ресурсов организации[2]. Политика информационной безопасности является объектом стандартизации (см. рисунок).

одно из наиболее актуальных и динамично развивающихся направлений стратегического и оперативного менеджмента в области информационной безопасности. Его основная задача - объективно идентифицировать и оценить наиболее значимые для бизнеса информационные риски компании, а также адекватность используемых средств контроля рисков для увеличения эффективности и рентабельности экономической деятельности компании. Поэтому под термином “управление информационными рисками” обычно понимается системный процесс идентификации, контроля и уменьшения информационных рисков компаний в соответствии с определенными ограничениями российской нормативной правовой базы в области защиты информации и собственной политики информационной безопасности.

Целью разработки политики информационной безопасности организации является

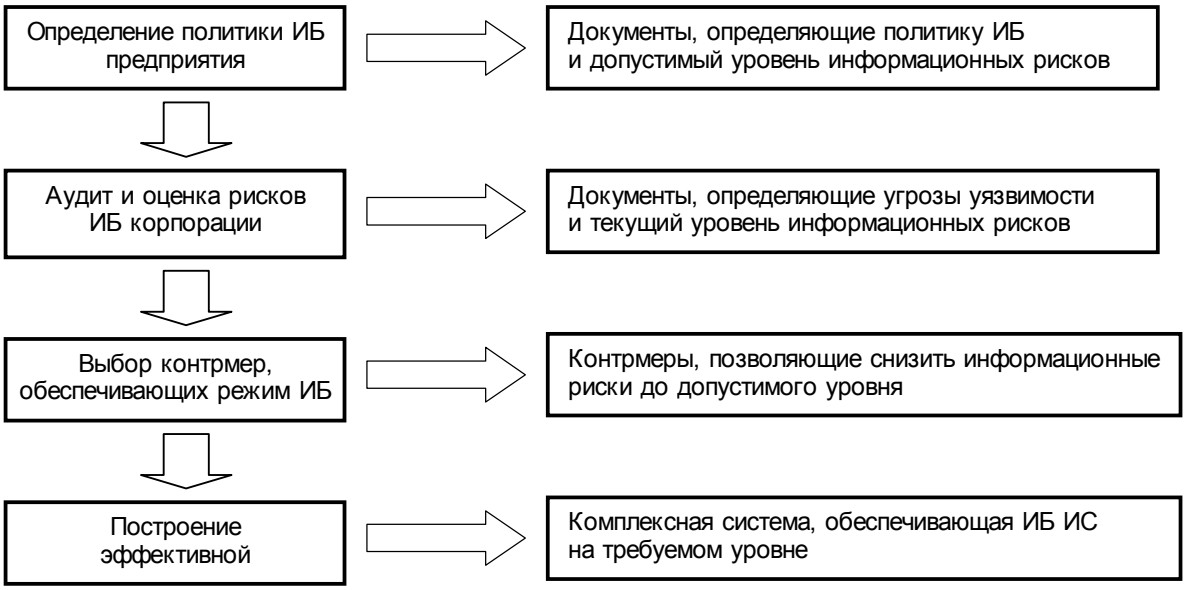

Рис. **Взаимосвязь ключевых задач управления ИБ**

Целью разработки политики информационной безопасности организации является определение правильного (с точки зрения организации) способа использования информационных ресурсов, а также разработка процедур, предотвращающих или реагирующих на нарушения режима, при этом, одной из ключевых задач политики информационной безопасности является определение уровня допустимого информационного риска.

В настоящее время управление информационными рисками представляет собой одно из наиболее актуальных и динамично развивающихся направлений стратегическо-

го и оперативного менеджмента в области информационной безопасности. Его основная задача - объективно идентифицировать и оценить наиболее значимые для бизнеса информационные риски компании, а также адекватность используемых средств контроля рисков для увеличения эффективности и рентабельности экономической деятельности компании. Поэтому под термином "управление информационными рисками" обычно понимается системный процесс идентификации, контроля и уменьшения информационных рисков компаний в соответствии с определенными ограничениями российской нормативной правовой базы в области защиты информации и собственной политики информационной безопасности.

Обеспечение информационной безопасности - это непрерывный процесс, основное содержание которого составляет управление: людьми, рисками, ресурсами, средствами защиты и т.д. Люди - обслуживающий персонал и конечные пользователи информационных систем являются неотъемлемой частью автоматизированной (т.е. "человеко-машинной") системы. От того, каким образом они реализуют свои функции в системе, существенно зависит не только ее эффективность (эффективность решения задач), но и ее безопасность.

Таким образом, научные исследования, направленные на повышение эффективности управления промышленным предприятием на основе формирования системы информационной безопасности, способной обеспечить согласованность действий, являются актуальными.

---

[1] *Балановская А.В.* Обеспечение информационной безопасности предприятий промышленности // Вестн. Самар. гос. ун-та. Самара, 2011. № 2. С. 72-78.

[2] *Грибунин В.Г., Чудовский В.В.* Комплексная система защиты информации на предприятии: учеб. пособие для студентов высш. учеб. заведений. М., 2009. С. 36-41.

Поступила в редакцию 15.03.2011 г.