УДК 351.862.4

С.Е. ЛОШАКОВА, ст. преп. НТУ "ХПИ"
Ю.В. НЕМЫКИНА, студент НТУ«ХПИ»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ДЕЯТЕЛЬНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

Статья посвящена определению видов информации, раскрытию понятия «конфиденциальная информация». Обоснована важность защиты информации для обеспечения её сохранности, целостности и безопасности. Предложен комплексный подход, который может обеспечить полную и надежную защиту информации промышленного предприятия.

The article is devoted determination of types of information, opening of concept «Confidential information». Importance of defence of information is grounded for providing of its safety, integrity and safety. Complex approach which can provide complete and reliable defence of information for industrial enterprise is offered.

Введение. В современном мире информация стала одним из наиболее мощных рычагов экономического развития. Владение информацией необходимого качества в нужное время и в нужном месте является залогом успеха во многих видах деятельности промышленных предприятий. Монопольное обладание определенной информацией оказывается зачастую решающим преимуществом в конкурентной борьбе.

Постановка проблемы. Проблема создания и поддержания защищенной среды информационного обмена, реализующая определенные правила и политику безопасности современной организации, является весьма актуальной. Информация давно уже перестала играть вспомогательную роль, превратившись в весьма важный и весомый фактор со своими стоимостными характеристиками, определяемыми той реальной прибылью, которую можно получить от ее использования. В то же время, вполне возможен и вариант получения ущерба, наносимого владельцу информации (предприятию) путем несанкционированного проникновения в информационную структуру и воздействия на ее компоненты. Из этого очевидно, насколько актуален в наши дни вопрос с защитой информации и информационных систем промышленных предприятий.

Анализ существующих разработок. Теоретической и методологической базой исследования являются работы российских и украинских авторов. Следует отметить работы таких авторов, как Духов В., Деревянко Е., Лагода Т. - определили информацию и информационную безопасность как одну из новых, но очень важных тем в деловых кругах. Конев И. и Беляев А. рассмотрели технологию информационной безопасности [1]. Садерлинов А.А. и Трайнев В.А. в своих трудах изложили системный подход к

построению комплексной защиты информационной системы предприятия [2].

Результаты исследований. Для формирования комплексной защиты информационной системы промышленного предприятия необходимо:

- рассмотреть существующие виды информации, показать её значение для предприятия;
- определить какая информация может относиться к коммерческой тайне;
- выяснить возможные потери от несанкционированного использования защищенной информации.

Один из главных составляющих факторов информационной безопасности - коммерческая тайна. Предметом коммерческой тайны является определенная информация и ее носители, которые являются следствием деятельности предприятия и приносят ему дополнительную прибыль, или укрепляют имидж. Предметом могут быть сведения, материалы, средства производства, технологии, организация труда, и тому подобное.

Как ни странно, в настоящее время не многие руководители предприятий осознают насущную необходимость в организации на предприятии системы защиты коммерческой тайны.

По категориям конфиденциальности основные виды информации распределяются следующим образом:

- деловая информация (сведения о контрагентах; сведения о конкурентах; сведения о потребителях; сведения о деловых переговорах; коммерческая переписка; сведения о заключенных и планируемых контрактах);
- научно-техническая информация (содержание и планы научно-исследовательских работ; содержание “ноу-хау”, рационализаторских предложений; планы внедрения новых технологий и видов продукции);
- производственная информация (технология; планы выпуска продукции; объем незавершенного производства и запасов; планы инвестиционной деятельности);
- организационно-управленческая информация (сведения о структуре управления фирмой не содержащиеся в уставе; оригинальные методы организации управления; система организации труда);
- маркетинговая информация (рыночная стратегия; планы рекламной деятельности; планы обеспечения конкурентных преимуществ по сравнению с продукцией других фирм; методы работы на рынках; планы сбыта продукции; анализ конкурентоспособности выпускаемой продукции);
- финансовая информация (планирование прибыли, себестоимости; ценообразование – методы расчета, структура цен, скидки; возможные источники финансирования; финансовые прогнозы);
- информация о персонале фирмы (личные дела сотрудников; планы увеличения (сокращения) персонала; содержание тестов для проверки вновь принимаемых на работу);

- программное обеспечение (программы; пароли, коды доступа к конфиденциальной информации, расположенной на электронных носителях).

Но следует учитывать, что приведенная классификация не является идентичной для всех предприятий, каждое предприятие строго индивидуально определяет, какая информация может быть общедоступной, а какая конфиденциальной.

Как правило, именно перечисленная выше информация в наибольшей степени интересует конкурентов, недобросовестных партнеров, банки, криминальные структуры.

Рассмотрим возможные последствия атак на информацию промышленных предприятий. Важнее всего, конечно, экономические потери. Во-первых, раскрытие коммерческой информации может привести к серьезным прямым убыткам на рынке. Во-вторых, известие о краже большого объема информации серьезно влияет на репутацию предприятия. В-третьих, предприятия-конкуренты могут воспользоваться кражей информации для полного разорения предприятия, навязывая ему фиктивные или заведомо убыточные сделки. В-четвертых, подмена информации как на этапе передачи, так и на этапе хранения на предприятии может привести к огромным убыткам. В-пятых, многократные успешные атаки на предприятие, предоставляющее и информационные услуги, снижает доверие к предприятию у клиентов.

Такие посягательства на информацию могут нанести существенный экономический ущерб промышленному предприятию, поэтому необходимо организовать комплексную систему защиты информации.

Так для разработки документов, затрагивающих вопросы работы с конфиденциальной информацией, необходимо в первую очередь разработать «Положение о конфиденциальной информации». Неотъемлемым приложением к Положению является Перечень документов, содержащих конфиденциальную информацию.

Для внедрения комплексной системы защиты информации необходимо создать Службу защиты информации, к задачам которой будут относиться:

- принятие мер по сохранению коммерческой тайны путем максимального ограничения круга лиц, физической сохранности документов, содержащих такие сведения,
- обработка информации с грифом конфиденциальности на защищенных ЭВМ,
- внесение требований по конфиденциальности конкретной информации в договоры с внутренними и внешнеторговыми партнерами и других мер по решению руководства,
- своевременное выявление угроз защищаемой информации предприятия, причин и условий их возникновения и реализации,
- выявление и максимальное перекрытие потенциально возможных каналов и методов несанкционированного доступа к информации,

- отработка механизмов оперативного реагирования на угрозы, использование юридических, экономических, организационных, социально-психологических, инженерно-технических средств и методов выявления и нейтрализации источников угроз безопасности предприятия,
- организация специального делопроизводства, исключающего несанкционированное получение конфиденциальной информации.

Вывод. Информация нуждается в защите в целях сохранения экономической стабильности промышленного предприятия. Максимальную эффективность обеспечения информационной безопасности промышленного предприятия может гарантировать только комплексная система защиты, так как системность обеспечивает необходимые составляющие информационной безопасности и устанавливает между ними логическую и технологическую связь. Именно комплексный подход может обеспечить полную и надежную защиту информации.

Список литературы: 1. *Конеев И. Р., Беляев А.В.* Информационная безопасность предприятия. - СПб.: БХВ - Петербург, 2003. - 752с. **2.** *Садерлинов А.А., Трайнев В.А., Федулов А.А.* Информационная безопасность предприятия: Учебное пособие. - 2-е изд. - М., Издательско-торговая корпорация "Даликов и К" 2005. - 336с.

Надійшла до редколегії 25.11.10