МАТЕМАТИЧЕСКИЕ И ИНСТРУМЕНТАЛЬНЫЕ МЕТОДЫ ЭКОНОМИКИ

УДК 65.012.45

А.В. Казакова*

КОНЦЕПЦИЯ ИНОФРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

Обосновывается необходимость разработки концепции информационной безопасности предприятия, исследуются принципы ее построения. Рассматриваются основные направления обеспечения информационной безопасности промышленных предприятий, организационная и инженерно-техническая защита.

Ключевые слова: информационная безопасность, концепция, информационная защита, информационные угрозы, информационная система.

Постоянный рост темпов развития и распространения информационных технологий, высокая конкуренция и существующая криминогенная обстановка ставят вопрос о создании на предприятии единой, соответствующей всем современным требованиям системы информационной безопасности (ИБ). Для предприятия она должна включать и увязывать в себе правовые, организационные, физические, инженерно-технические и программные направления обеспечения защиты информационных ресурсов.

Для полной оценки ситуации на предприятии по всем направлениям обеспечения ИБ необходима разработка Концепции информационной безопасности (далее – Концепция), которая бы устанавливала системный подход к проблеме безопасности информационных ресурсов и представляла собой систематизированное изложение целей, задач, принципов проектирования и комплекса мер по обеспечению ИБ на предприятии (рис. 1).

При разработке следует учитывать современные организационные, правовые методы и программно-технические средства противодействия внешним и внутренним угрозам ИБ, а также существующее состояние защищенности информации и перспективы развития информационных технологий.

Основные правила и требования Концепции ИБ распространяются на всех сотрудников предприятия, так или иначе связанных с обработкой, хранением, под-

Казакова Арина Валерьевна (arina-21@mail.ru), кафедра экономики промышленности Самарского государственного экономического университета, 443090, Российская Федерация, г. Самара, ул. Советской Армии, 141.

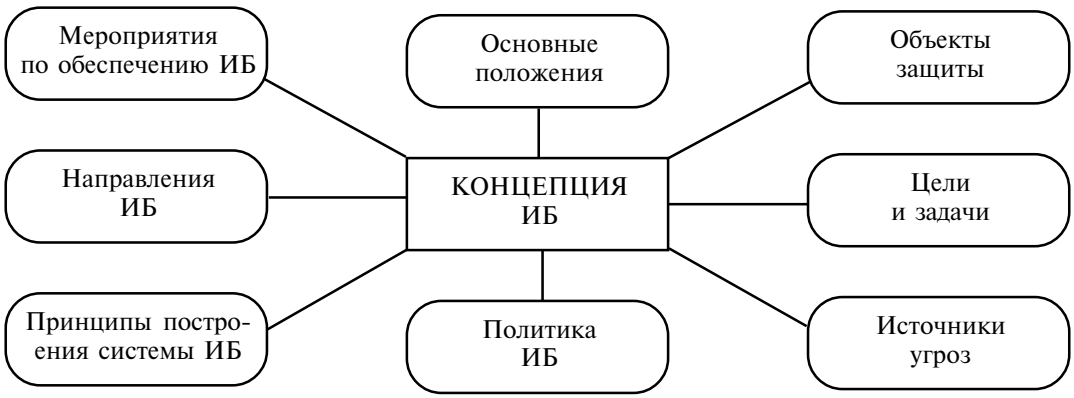

Рис. 1. Концепция информационной безопасности предприятия

держкой или созданием информационных ресурсов, требующих обеспечения их целостности, конфиденциальности и доступности, а также на лиц сторонних организаций, отвечающих за обновление или поддержку программного обеспечения.

Концепция служит основой для создания единой политики обеспечения ИБ на предприятии; координации деятельности структурных подразделений компании; принятия решений и проведения мероприятий, направленных на предотвращение, выявление и устранение последствий различных угроз; поиска новых решений, направленных на совершенствование обеспечения ИБ.

Объектами защиты на предприятии являются сотрудники, финансовые средства, материальные ценности, информационные ресурсы с ограниченным доступом, представляющие коммерческую, технологическую или иную тайну, а также общедоступная информация вне зависимости от формы и вида ее представления; информационная система, состоящая из программных и технических средств обработки и анализа информации, передачи и отображения, каналов информационного обмена, средств защиты информации, помещений; репутация фирмы.

Структура и состав информационной системы для большинства современных предприятий представляют собой в основном совокупность технических и программных средств обработки данных (ПК, серверы и т. п.), средств обмена данными с возможностью выхода в Интернет, средств хранения данных. Особенностями функционирования современных информационных систем являются следующие: применение в единой системе различных технических средств обработки и передачи информации; использование единых баз данных для информации различного назначения и уровня конфиденциальности; доступ к информационным ресурсам пользователей разных категорий и обслуживающего персонала; наличие каналов взаимодействия с глобальной сетью; постоянное функционирование информационной системы.

В информационной системе предприятия находится в постоянном движении всевозможного рода информация, принадлежащая к различным уровням конфиденциальности и несущая в себе сведения ограниченного или свободного распространения.

Основной целью Концепции ИБ является защита субъектов информационных отношений от возможного нанесения им материального, морального или иного ущерба из-за преднамеренных или случайных действий с информационными ресурсами, результатом которых выступает потеря их свойств, таких как доступность, целостность и конфиденциальность.

Задачи Концепции ИБ состоят в обеспечении защиты существующей информационной инфраструктуры предприятия от вмешательства злоумышленников,

условий для локализации и минимизации возможного ущерба, выявлении на начальной стадии причин возникновения источников угроз. Решение вышеназванных задач достигается путем четкого категорирования информационных ресурсов компании; регламентации действий сотрудников; подготовки лиц, ответственных за обеспечение и соблюдение ИБ; строгого выполнения и знания сотрудниками предприятия свода правил и требований по обеспечению ИБ; использования программно-технических средств защиты информации; правовой и физической защиты; постоянного контроля и анализа эффективности, необходимости используемой системы защиты и принимаемых мер.

Источниками угроз ИБ могут быть как случайные действия сотрудников, так и преднамеренные со стороны нелояльного к деятельности предприятия персонала. Особо отметим возможные неправомерные действия со стороны конкурентов, партнеров по бизнесу или криминальных структур, способных образовывать группы с привлечением как действующих, так и уволенных сотрудников предприятия. Подобные альянсы несут максимальную угрозу системе ИБ. Также источником угроз могут быть действия спецслужб, государственных чиновников, хакеров, техногенные и природные факторы.

Под политикой ИБ понимается совокупность документированных управленческих решений, направленных на защиту информационных ресурсов предприятия, что в свою очередь обеспечивает эффективное управление и поддержку политики в области ИБ со стороны руководителей предприятия. Задачами вышеназванной политики выступают выбор оптимального способа использования информационных ресурсов, а также разработка процедур, предотвращающих или реагирующих на нарушения режима безопасности [1].

Политика ИБ компании является объектом стандартизации, поэтому многие страны имеют национальные стандарты, определяющие основное содержание подобных документов. К сожалению, многие вопросы по ИБ в отечественных руководящих документах не рассмотрены. Поэтому при разработке политики ИБ фирмам целесообразно использовать более совершенные и современные зарубежные стандарты, позволяющие разработать более качественные документы.

При построении системы информационной безопасности предприятия необходимо придерживаться определенных принципов (см. таблицу).

Таблица

Принципы обеспечения информационной безопасности

Принцип	Содержание
Законность	подразумевает, что проектирование системы ИБ и осуществление мер по защите информационных ресурсов выполняются в соответствии с действующим законодательством и нормативными актами по ИБ, утвержденными органами государственной власти РФ. Предприятие должно использовать только дозволенные методы обеспечения ИБ
Системность	предполагает единый системный подход к проектированию системы ИБ, учитывая все многообразие типов связей между различными элементами, факторами и обстоятельствами, значимыми для понимания и решения вопросов по обеспечению ИБ на предприятии. При создании системы ИБ следует учитывать пути реализации угроз, объекты несанкционированных действий, уязвимости
Комплексность	заключается в том, что для построения системы ИБ необходимо использовать согласованный комплекс мер и средств защиты, перекрывающих все возможные источники угроз

Окончание таблицы

Принцип	Содержание
Непрерывность	связана с тем, что защита информации и информационной инфраструктуры предприятия – это процесс непрерывный, требующий четкого и постоянного соблюдения намеченных правил и мер на всех этапах существования системы ИБ. Поскольку для большинства аппаратно-технических и программных средств требуется постоянная и своевременная административная поддержка, даже незначительный простой средств защиты может быть использован злоумышленниками для реализации своих угроз
Целесообразность	подразумевает сопоставление уровня затрат и величины вероятного ущерба от потери основных свойств информации. Система ИБ должна быть разумной, экономически эффективной и не мешать нормальному функционированию информационной системы, в которой циркулирует защищаемая информация. При проектировании системы защиты важно учитывать, что полностью исключить вероятность нанесения ущерба невозможно, можно лишь ее снизить
Гибкость	состоит в возможности системы ИБ оперировать уровнем защищенности, а также быть удобной для модернизации по мере устаревания. Контроль предполагает своевременное выявление и пресечение попыток несоблюдения персоналом предусмотренных системой ИБ мер и средств
Простота	подразумевает, что используемые механизмы реализации защиты информационных ресурсов должны быть интуитивны, не требовать от рядовых пользователей особых знаний, лишних и раздражающих действий. Все сотрудники или лица сторонних организаций, участвующие в создании и реализации механизмов защиты информационных ресурсов, должны быть максимально подготовлены, иметь опыт работы, т. е. быть профессионалами в своей области
Ответственность	за обеспечение ИБ ответственность возлагается на каждого сотрудника в пределах его полномочий. Это необходимо для сужения круга виновных лиц в результате реализации угроз информационным ресурсам

По мнению ряда специалистов, существует некоторое оптимальное значение затрат на ИБ, минимизирующее общий ущерб (рис. 2).

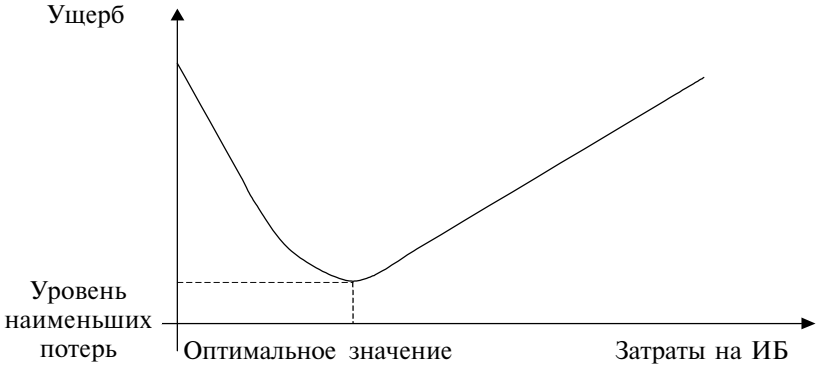

Рис. 2. Зависимость уровня ущерба от уровня затрат на ИБ

Поэтому необходимо выбрать тот достаточный уровень защищенности информационных ресурсов, при котором уровень затрат на обеспечение ИБ и вероятный ущерб были бы приемлемы.

По их мнению, даже применение относительно недорогих способов и средств обеспечения ИБ (антивирусные программы, организационные ограничения и т. д.) резко снижает общий ущерб. Поэтому затраты на ИБ в сравнительно малых размерах весьма эффективны в небольших организациях, не подвергающихся специаль-

ным компьютерным атакам. При этом кривая имеет оптимальное (наименьшее) значение.

С учетом существующей практики выделим основные направления обеспечения ИБ на предприятии, а именно правовую, организационную и инженерно-техническую защиту.

Правовую основу ИБ предприятия следует делить на внешнюю и внутреннюю защиту (рис. 3).

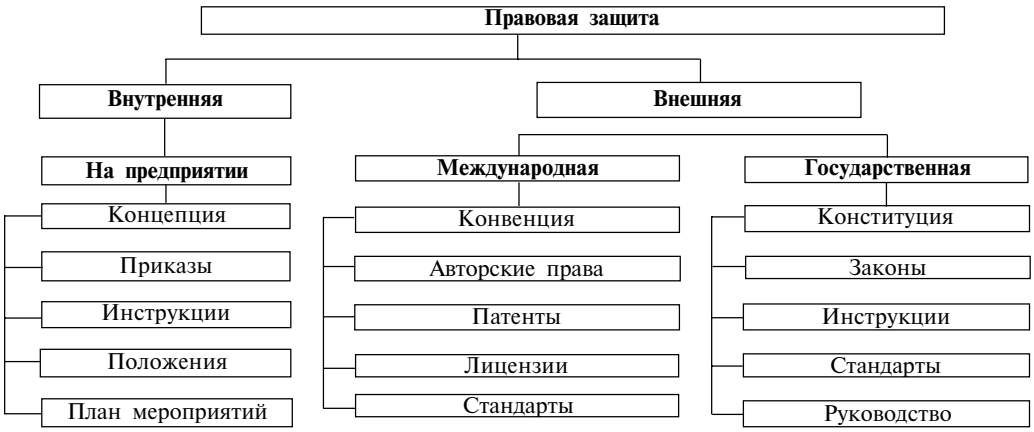

Рис. 3. Правовые основы ИБ

К внешней мы относим те правовые аспекты деятельности, на состав и содержание которых предприятие никаким образом повлиять не может, тем самым повысив свое состояние защищенности. К этому уровню относятся нормы международного и государственного права.

Под внутренней правовой защитой понимают специальные правила, акты, мероприятия, процедуры, приказы, которые определяет, разрабатывает, регулирует и контролирует само предприятие, обеспечивая тем самым внутреннюю политику ИБ.

Организационная защита предполагает регламентацию деятельности предприятия по следующим направлениям организации: режима и охраны; работы с персоналом (подбор персонала, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил, мотивация); работы с документами (организация составления и использования документов, их учета, хранения, уничтожения); использования технических средств сбора, обработки, хранения информации; работы по анализу внутренних и внешних угроз конфиденциальной информации и разработке мер по ее защите; регулярного контроля за работой персонала с конфиденциальной информацией. Организационная защита играет большую роль в обеспечении ИБ предприятия (рис. 4).

Чаще всего утечка информации и несанкционированный доступ к ней связаны со злоумышленными действиями, небрежностью сотрудников. Эти ситуации очень трудно предотвратить с помощью технических, физических средств защиты. Важным организационным мероприятием по обеспечению ИБ на предприятии выступает создание специальных штатных единиц по защите информации (или служб безопасности).

Инженерно-техническая защита – совокупность мероприятий с использованием физических, программно-технических средств, персонала в целях защиты информации (рис. 5).

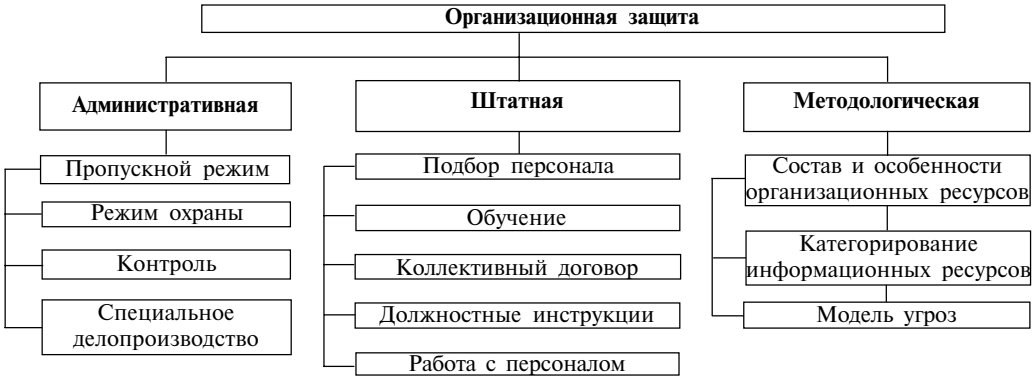

Рис. 4. Организационные основы ИБ

Рис. 5. Инженерно-технические основы ИБ

Охранно-пожарная сигнализация предназначена для обнаружения проникновения в помещение человека, движения на объекте, целостности окон, стен, решеток, открытия дверей или возникновения пожара в помещении и информирования об этом событии поста охраны, который, в свою очередь, принимает необходимые меры по ликвидации данного события.

Система видеонаблюдения – это постоянный визуальный мониторинг и запись на магнитные или цифровые носители информации о ситуации на охраняемом объекте с централизованного поста охраны. Она позволяет контролировать входы на территорию предприятия, в здания, отдельные кабинеты. При необходимости система видеокамер может устанавливаться непосредственно в комнатах, что позволяет вести наблюдение за происходящим в помещении.

Система бесперебойного питания и резервных аккумуляторов обеспечивает работоспособность всех сигнализационных, видео, контрольных и компьютерных

систем при пропадании напряжения в электрической сети. Система контроля доступа – это ограничение прохода людей в определенное помещение, сбор и запись информации о прошедших через определенный проход людей (время, количество проходов, ФИО и т. д.). Все системы могут быть объединены в комплексную систему безопасности, в том числе с применением компьютерных сетей и с возможностью удаленного доступа (просмотр изображений видеокамер, управление, конфигурирование). Физическая защита территории заключается в установке заборов. Защита здания осуществляется путем установки решеток, пуленепробиваемых стекол, дверей. Помещения должны обязательно запираться на ключ, при необходимости опечатываться.

Кратко охарактеризуем самые распространенные программно-технические средства защиты информации на предприятиях.

Антивирусное программное обеспечение служит для обнаружения компьютерного вируса, а также корректного лечения зараженного объекта, восстанавливая его в первоначальном виде в случае невозможности удаления зараженного файла. Резервное копирование является оптимальным решением по обеспечению высокой доступности информации и предназначено для создания резервных копий и восстановления данных.

Идентификация представляет собой процесс назначения субъектам или объектам доступа уникального признака, т. е. идентификатора. Аутентификация — это процесс проверки подлинности идентификатора предъявляемого субъектом доступа. Шифрование информации применяется для обеспечения невозможности ее прочтения злоумышленниками. Оно особенно актуально при передаче конфиденциальной информации или записи на магнитный носитель. Экранирование подразумевает использование межсетевых экранов, обеспечивающих безопасность работы внутренней сети, игнорируя несанкционированные запросы из внешней сети. Как правило, оно является необходимым элементом при работе с глобальными сетями.

Протоколирование и аудит предполагают защиту информации путем регистрации действий пользователей, фиксации изменений паролей и различных параметров системы, выявления несанкционированных действий для проведения дальнейшего анализа и принятия решений. Электронно-цифровая подпись обеспечивает получателю гарантированную подлинность полученной информации и достоверность факта ее оправки от имени, указанного в письме отправителя.

Завершая рассмотрение концептуальных основ построения системы ИБ предприятия, отметим, что, на наш взгляд, самым важным принципом построения является целесообразность, т. к. ее отсутствие делает бесполезным все иные шаги по созданию системы ИБ. Поэтому исследованию компонентов, характеризующих целесообразность, будет уделено особое внимание. Так, для выявления достаточного уровня защищенности информационных ресурсов особенно актуальным является изучение на предприятии методологических составляющих организационной защиты ИБ, а именно состава и особенностей информационных ресурсов на фоне имеющихся угроз.

Библиографический список

1. Минаев В.А., Карнычев В.Ю. Цена информационной безопасности // Информационная безопасность. 2003. Декабрь. С. 26.

A.V. Kazakova*

CONCEPT OF INFORMATION SECURITY OF ENTERPRISES

Necessity of working out the concept of information security of the organization is proved, principles of its construction are investigated. The basic directions of maintenance of information security of the industrial enterprises are considered: organizational and technical protection.

Key words: information security, concept, information protection, information threats, information system.

* *Kazakova Arina Valerievna* (arina-21@mail.ru), the Dept. of Industrial Economics, Samara State University of Economics, Samara, 443090, Russian Federation.