[Электронный ресурс] // Режим доступа: http://www.twirpx.com/file/1391064/ (Дата обращения 10.05.2014).
3. Программа арктического мониторинга и оценки. Итоговые рекомендации: борьба с краткосрочными факторами арктического потепления и таяния северных льдов [Электронный ресурс] // Режим доступа: http://www.bellona.ru/filearchive/fil_AMAPSummary_Recommendations-RUS.pdf (Дата обращения 10.05.2014).
4. Тишков, А.А. «Арктический вектор» в сохранении наземных экосистем и биоразнообразия [Текст] // Арктика: экология и экономика. 2012. №2 (6). С.32.
5. Доклад о развитии человека в Арктике [Текст] / под ред. А.В. Головнёва. – Екатеринбург, Салехард, 2007. – 244 с. С. 229.
6. Силин, А.Н. Нефтегазовый Север: социальная ситуация и технологии ее регулирования: Монография [Текст] / А.Н. Силин. – М.: ИНФРА-М, 2013. – 251 с. С.27.

ФОРМИРОВАНИЕ КОМПЛЕКСНОЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК ВАЖНЕЙШИЙ ЭЛЕМЕНТ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

С.А. Борисов
Нижегородский государственный технический университет им. Р.Е. Алексеева

В статье рассмотрены основные и инновационные меры по обеспечению комплексной защищенности информационных систем на промышленных предприятиях. Анализируется проблемы формирования комплексной системы защиты информации, как сложной социотехнической системы. Выделены основные функции и рассмотрены мероприятия по формированию комплексной системы защиты информации на предприятии.

Ключевые слова: экономическая безопасность, информационные системы, биосоциальный, технический и программный компоненты, коммерческая тайна, угрозы, система.

В настоящее время большинство предприятий, как крупного масштаба, так и средние и мелкие организации активно используют в своей деятельности автоматизированные информационные системы (ИС). Они необходимы предприятиям для создания единого информационного пространства, обеспечивающего эффективное взаимодействие как внутри предприятия, так и его взаимодействие с другими организациями. ИС используется внутри организации для предоставления сотрудникам определенных информационных сервисов, обеспечения совместной работы в рамках единого информационного пространства с учетом специализации каждого сотрудника, автоматизации различных операций, производимых сотрудниками (в том числе в области производства, финансов, маркетинга и т.д.). С использованием современных ИС происходит эффек-

тивное управление и контроль над бизнес-процессами, протекающими в различных отделах предприятия. В области взаимодействия предприятия с другими организациями ИС выполняют следующие функции: предоставляют возможность быстрого обмена данными с использованием сервисов электронной почты, теле и видеоконференций, возможности вести работу над одним проектом организациям, распределенным во времени и пространстве. Таким образом, автоматизированные ИС, несомненно, являются важным помощником современной организации как в исполнении их рутинных бизнес-процессов, так и в проектах, направленных на совершенствование деятельности организации в будущем. Вместе с тем, ИС, рассматриваемая как стратегический актив организации, имеет и «обратную сторону медали», заключающуюся в том, что при ее неправильном или сознательно неправомерном применении вместо положительных эффектов от ее использования, рассмотренных выше, возникают специфические угрозы для предприятия. Спектр этих угроз может быть достаточно широк – от неумелых действий пользователя до сознательных методов взлома и хищения информации. Соответственно, ущерб от данных противоправных действий также может существенно различаться и может выражаться в потери части прибыли из-за передачи части конфиденциальной части информации конкурентам (раскрытие коммерческой тайны), в потере стратегического конкурентного преимущества. Особенно серьезными являются нарушения, связанные с разглашением государственной, военной тайны, которые ведут не только к крайне негативным последствиям для конкретного предприятия, но и в существенной мере затрагивают интересы национальной безопасности государства.

Соответственно, для того, чтобы обезопасить предприятие от широкого спектра информационных угроз, необходима разработка определенных мер защиты информации, позволяющих обеспечить ИБ предприятия. В настоящее время разработано достаточно большое количество подходов к обеспечению ЗИ на предприятии. Программистами разработаны специализированные подходы к ЗИ на уровне аппаратного и программного обеспечения для ЭВМ, организационными службами предприятия разрабатываются меры по ограничению доступа к определенным категориям информационных ресурсов. Вместе с тем, совершенствование информационной безопасности (ИБ), проводимое на уровне отдельных категорий, в большинстве случаев оказывается недостаточно эффективными, остаются существенные пробелы в области защиты информации (ЗИ) на предприятии. Таким образом, необходимо совершенствование различных аспектов ЗИ в рамках единой системы, которая бы не просто сочетала в себе элементы различных направлений ИБ, а учитывала взаимосвязи между ними, использовала положительный опыт, накопленный в рамках одного направления и при наличии соответствующей возможности переносила его на другие методы защиты ИБ на предприятии.

Системой, обеспечивающей эффективное совместное развитие средств ЗИ на предприятии, выступает комплексная система ЗИ. Формирование такой системы на предприятии позволяет в рамках единых организационно – методологических подходов проводить совершенствование конкретных методов

ЗИ на предприятии [1]. При формировании данной системы необходимо учитывать два важнейших обстоятельства:

1) главным элементом системы ЗИ выступает человек. Вместе с тем, он, как правило, является наиболее слабоформализуемым и уязвимым звеном системы;

2) в отличии от производства продукции или получения прибыли, ЗИ не выступает в качестве главной задачи предприятии. Поэтому, при построении такой системы необходимо учитывать следующие обстоятельства:

- создаваемая система для обеспечения ЗИ не должна существенно усложнять сотрудникам предприятия выполняемые ими рабочие функции;
- внедрение системы ЗИ должно быть экономически целесообразным.

При этом, сформированная система ЗИ должна эффективно бороться с широким спектром информационных угроз, возникающих перед предприятием. Сегодня большинство руководителей и сотрудников организаций понимают, что отдельные разрозненные мероприятия по ЗИ не способны обеспечить надежную ИБ в свете постоянного увеличения и усложнения различных информационных угроз. Таким образом, создание комплексной системы ЗИ фактически признается организациями как условие эффективного существования и дальнейшего развития компании. Основной вопрос состоит не в том, нужно ли создание такой единой системы ЗИ, а в том, каким образом эта система должна быть организована. При этом, как было указано ранее, необходимо что система ЗИ была одновременно и эффективным защитником от возникающих информационных угроз, но при этом не мешала бы сотрудникам осуществлять свою деятельность. Систему ЗИ можно представить в виде трех взаимодействующих групп систем [1]: 1) биосоциальные системы (персонал организации); 2)техника – технические системы и помещения, в которых они расположены; 3) программное обеспечение (ПО), которое выступает в качестве посредника между биосоциальной системой и технической системой. Как правило, на текущий момент развития и техники, в качестве программного обеспечения выступают интеллектуальные ИС. Таким образом, комплексная система ЗИ представляет собой сложную социотехническую систему.

Наибольшей эффективностью данная система будет обладать в том случае, если будут разработаны специальные механизмы защиты, и в процессе формирования комплексной системы будет происходить непрерывное управление данными механизмами. Основными функциями комплексной системы ЗИ должны выступить следующие:

1. Функция по созданию механизмов защиты, сводящая к минимуму возможность воздействия на защищаемые ресурсы в ИС организации.

В рамках реализации данной функции должны быть решены следующие задачи: а) созданы и поддерживаются в актуальном состоянии механизмы защиты, сводящие к минимуму вероятность появления дестабилизирующих факторов; б) система действий «на опережение» при появлении благоприятных условий для возникновения информационных угроз; в)своевременное обнаружение воздействия дестабилизирующих факторов на информацию с возможностью

последующей ликвидации информационных угроз в как можно более короткий промежуток времени.

2. Функция непрерывного и оптимального управления механизмами комплексной защиты. В данном случае под управлением понимается обеспечение сохранения определенной структуры, поддержания режимов деятельности, реализации программ и целей подсистем комплексной системы защиты информации (биосоциальный, технический и программный компоненты). При реализации рассматриваемых функций необходимо учитывать следующие особенности современного предприятия, защита данных которого и является основной целью создания и поддержания комплексной системы защиты информации:

1) многие современные предприятия обладают сложной организационной структурой;

2) наличие на предприятии большого количества разнородных аппаратных средств и программного обеспечения;

3) непрерывно расширяющаяся деятельность (открытие новых продуктовых линеек, офисов, дочерних предприятий, расширяющееся взаимодействие с клиентами и партнерами);

4) перевод значительной части документов в электронный вид, применение электронной цифровой подписи;

5) передача информации предприятия с использованием различных каналов коммуникации, в том числе спутниковых каналов.

Данные особенности современного предприятия, а также увеличение общего роста компьютерных преступлений в мире, требуют постоянных мер не только по поддержанию текущего уровня ЗИ, но и непрерывного совершенствования комплексной системы ЗИ на предприятии.

Для того, чтобы перейти к рассмотрению конкретных мероприятий по формированию комплексной системы ЗИ на предприятии, необходимо сначала более подробно рассмотреть сам объект защиты, то есть, какие виды информации подлежат защите. В качестве информации, подлежащей защите, выступают следующие категории [2]: персональные данные сотрудников организации, хранящиеся в локальной БД организации и которые могут быть переданы посредством коммуникационных каналов; сообщения электронной почты, в которых содержатся служебные сведения, информация о деятельности предприятия; конструкторская и технологическая документация предприятия, в том числе перспективные планы развития, финансовая информация, результаты маркетинговых исследований компании (в том числе о рынках, конкурентах и т.д.) и др. К строго конфиденциальным сведениям относятся стратегические планы компании, разглашение которых может привести к срыву основных функций предприятия, влияющих на обеспечение его жизнеспособности и развития, а в худшем случае сведений может даже привести к полному краху предприятия. Исходя из важности охраняемых сведений и наступлением существенных негативных последствий в случае их разглашения, необходимо определить порядок организации и содержание работ по защите ИБ в рамках комплексной системы ЗИ, а также определить ответственных за обеспечение ИБ на каждом участке работы. При построении комплексной системы ЗИ необходимо учитывать раз-

личную приоритетность в ЗИ. Наивысшую ценность для предприятии составляет государственная тайна (эта категория может и отсутствовать на конкретном предприятии), на втором месте располагается коммерческая тайна – информация, которая приносит определенную ценность компании пока она известна только ограниченному кругу лиц; далее следует служебная тайна и персональные данные сотрудников, конфиденциальная информация, принадлежащая третьей стороне, а также данные, критичные для функционирования ИС и работы бизнес-подразделений. Согласно концепции ИБ [2], организация работ по обеспечению ИБ и ЗИ возлагается на руководителя департамента ИТ предприятия. Им осуществляется эксплуатация и сопровождение ИС. За методическое руководство и контроль над эффективностью предусмотренных мер ЗИ отвечает начальник службы ИБ предприятия. Желательно, чтобы указанные должности занимались различными сотрудниками. Эксплуатация ИС предприятия должна осуществляться в соответствии с утвержденной организационно – распорядительской документацией, эксплуатационной документацией, должны быть учтены положения государственных и международных стандартов, а также разработанные локальные акты по обеспечению ИБ и ЗИ в компании.

Основными мерами по обеспечению комплексной защищенности ИР на предприятии выступают:

1) разработка, реализация, внедрение и контроль исполнения планов мероприятий, политик безопасности и др.;
2) определение ролей и распределение ответственности использование ИР корпоративной сети;
3) совершенствование технической инфраструктуры системы организации ИБ;
4) мероприятия по подготовке рядовых пользователей и специалистов к решению проблем, связанных с обеспечением ИБ;
5) проведение аудита состояния ИБ на предприятии.

Комплексная система обеспечения ИБ на предприятии функционирует путем сочетания мер организационного и программного – технического уровней. Рассмотрим более подробно состав и функции организационных и программного – технических мер. Меры организационного уровня представлены следующими категориями: меры административного уровня и процедурные методы ЗИ. К первой группе относятся меры, основой которых является политика ИБ предприятия – совокупность документированных управленческих решений, направленных на ЗИ и ассоциированных с ней ресурсов [3]. Основными документами политики ИБ предприятия выступают следующие политики: защита от несанкционированного доступа к информации, управление паролями, использование электронной почты, анализа защищенности ИС и ИР предприятия; должностные инструкции для операторов, администраторов и инженеров, осуществляющих эксплуатацию и обслуживание ИС и др. К процедурному уровню относятся меры, осуществляемыми сотрудниками предприятия. В качестве таких мер выступают: управление персоналом (УП), физическая защита, реагирование на нарушение режима безопасности и др. УП предполагает включение в должностные инструкции разделов, касающихся ИБ, а также разработку квали-

фикационных требований для различных категорий сотрудников по обеспечению ИБ. Важным аспектом УП является ознакомление каждого работника со ст. 192 Трудового Кодекса РФ, согласно которому сотрудники, нарушающие требования политики безопасности предприятия, могут быть подвергнуты дисциплинарными взысканиям, таким как: замечание, выговор, увольнение с работы. За разглашение сведений, составляющих охраняемую законом тайну (государственную, коммерческую или иную), а также умышленное причинение ущерба, в случаях, предусмотренных федеральными законами, сотрудники предприятия несут материальную ответственность в полном размере причиненного ущерба (согласно ст. 243 Трудового Кодекса РФ).

В качестве мер по обеспечению физической защиты выступают: защита поддерживающей структуры, физическое управление доступом, обеспечение противопожарных мер безопасности. Реагирование на нарушение режима безопасности производится, главным образом, по двум направлениям: 1) блокирование нарушителя и уменьшение нанесенного вреда; 2) недопущение повторных нарушений. Для обеспечения таких мероприятий в организации должен быть выделен специально обученный сотрудник, который в режиме 24/7 должен быть ответственным за реакцию на нарушения, и все сотрудники должны иметь с ним связь.

В качестве средств защиты технического и программного уровня выступают следующие инструменты: 1) подсистема идентификации и аутентификации (обеспечивает поддержание идентичности и синхронизацию учетных данных в различных хранилищах, предоставляет единую точку доступа и администрирования, безопасный домен входа в ОС Windows при помощи электронного идентификатора); 2) подсистема разграничения доступа (использование специализированных серверов авторизации), 3) подсистема активного аудита безопасности (анализ сетевого трафика должен обнаруживать известные типы сетевых атак, включая атаки, направленные против следующих приложений: СУБД, Web, FTP, почтовые серверы, почтовые агенты, Web-браузеры и т.д.); 4) подсистема контроля целостности (должна обеспечивать контроль неизменности атрибутов критичных файлов и их содержимого, а также своевременное выявление нарушение их целостности и восстановление); 5) подсистема контроля защищенности (сетевой сканер должен обнаруживать уязвимости различных операционных систем, баз данных, сетевых сервисов и приложений). Также для обеспечения технической защищенности применяются такие средства, как: сегментирование и межсетевое экранирование, средства антивирусной защиты (в том числе серверов локальных вычислительных сетей, рабочих станций, почтовой системы и др.) и др. Таким образом, в настоящее время разработан широкий перечень мер программного и технического обеспечения ИБ. Вместе с тем, как было указано ранее в связи с наличием человека как активного элемента системы, эффективность рассмотренных мер существенно снижается без использования организационно – правовых и экономических мер по поддержанию ИБ и ЗИ.

Соответственно, разработка системы комплексной защищенности ИС на предприятии является одной из его важнейших задач, от решения которой зависит эффективность работы компании в настоящий момент и в будущем. В на-

стоящей статье приведены основные подходы к формированию системы комплексной защищенности ИР предприятия, а также отмечены основные особенности, которые нужно учитывать при построении данной системы.

Библиографический список

1. Попов, В.В. Курс лекций по дисциплине «Комплексная защита информации на предприятии». Московский авиационный институт (МАИ), 2009 [Электронный ресурс] // Режим доступа: http://securitypolicy.ru/index.php/ (Дата обращения: 19.02.2014)
2. Концепция обеспечения информационной безопасности Электронный ресурс] // Режим доступа: http://securitypolicy.ru/index.php/Концепция обеспечения информационной_безопасности_предприятия (Дата обращения: 19.02.2014).
3. Герасименко, В.А.Защита информации в автоматизированных системах обработки информации [Текст] / В.А. Герасименко. – М.: Энергоатомиздат, 1994. – 568с.
4. Колесов, К.И. Методологические аспекты стратегического контроллинга на основе многоуровневого подхода: монография [Текст] / К.И. Колесов, А.Ф. Плеханова. – Н.Новгород: НГТУ, 2010.
5. Колесов, К.И. Методические аспекты управления рисками на основе внедрения системы внутреннего контроля: статья [Текст] / К.И. Колесов, А.С. Антонов // Труды НГТУ им. Р.Е. Алексеева. 2013. №3. С. 272-278.

ПРОЕКТИРОВАНИЕ И ВНЕДРЕНИЕ ИНТЕГРИРОВАННЫХ ЦЕПЕЙ ПОСТАВОК КАК ФАКТОР ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

С.Б. Вдовина

Нижегородский государственный технический университет им. Р.Е. Алексеева

В статье рассмотрены вопросы реализация концепции интегрированной логистики на предприятии. Отмечены положительные тенденции при внедрении интегрированных цепей поставок. Рассмотрена общая идеология *SCOR*-модели, которая объединяет современные управленческие концепции: реинжиниринг бизнес-процессов, бенчмаркинг и использование наилучшей практики. Приведены показатели функционирования интегрированных цепей поставок, которые условно делятся на две категории: внешние (ориентированные на клиента) и внутренние (ориентированные на бизнес-процессы фокусной компании).

Ключевые слова: экономическая безопасность, планирование, модель и инструменты, *SCOR*-модель, конкурентные преимущества.