УДК 338.26:004.4

МЕХАНИЗМ РАЗРАБОТКИ ИННОВАЦИОННОГО ПРОЕКТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ

© 2015 А.В. Балановская*

Ключевые слова: информация, информационная безопасность, система информационной безопасности, инновационный проект, эффективность.

Представлены основные этапы построения системы информационной безопасности промышленного предприятия, обоснован инновационный подход к проектированию, дан анализ основ его реализации.

В современном мире происходит постоянное усовершенствование применяемых информационных технологий. Однако уязвимость защиты информационной системы предприятий не уменьшается, более того, следует отметить обратную тенденцию, при которой наблюдается процесс увеличения уязвимости защиты. На современных предприятиях все большее распространение получают автоматизированные информационные системы управления[1]. Именно поэтому перед промышленными предприятиями встает проблема обеспечения информационной безопасности.

Изучение многих подходов к решению проблемы формирования системы информационной безопасности позволяет нам предложить последовательность построения системы информационной безопасности предприятия, включающую ряд этапов.

На первом этапе, подготовительном, происходит выбор объекта, который может быть заявлен как информационная система в целом или ее отдельная подсистема, компонент и т.д.). Проводится комплексный анализ имеющихся ресурсов, выявляются ограничения, исследуются методы подготовки, приема, хранения, передачи и обработки информации, изучаются особенности архитектуры информационной системы организации, характер и ценность информации, обращающейся в информационной системе предприятия.

Одновременно приводится описание ресурсов системы, которые следует объединить в несколько категорий, таких как: данные; вычислительная и коммуникационная техника; персонал; программное обеспечение; дополнительные ресурсы.

На базе проведенного исследования в рамках подготовительного этапа разрабатывается общая концепция системы информационной безопасности промышленного предприятия. На данном уровне следует определить цели и задачи, сформировать основополагающие требования, которые будут учитывать не только результаты анализа текущей ситуации, но также и возможные перспективы развития потребностей, направления прогресса в сфере информатизации, новинки в области технологий обработки, хранения, обновления и передачи данных.

Далее планомерно осуществляется переход от подготовительного этапа ко второму этапу - аналитическому.

Основными задачами данного этапа являются изучение и количественное оценивание рисков, выявление и систематизация возможных угроз, поиск возможных каналов несанкционированного доступа, а также утечки информации, сбор информации об объектах, которые подлежат защите, и разработка обоснованных критериев эффективности защиты информации.

При исследовании угроз, возможных и потенциальных, важным является изучение информации, поступающей из внешней среды, и оценка ее на достоверность и определение степени полноты поступающей информации. Такая проверка на достоверность включает оценку различных источников информации, как первичных, так и вторичных. Изучаются периодические издания, научные конференции, специализированные публикации и т.д. Не менее важно учитывать внутреннюю информацию, касающуюся сообщений о конф-

* Балановская Анна Вячеславовна, кандидат экономических наук, доцент Самарского государственного экономического университета. E-mail: balanovskay@mail.ru.

ликтах, сбоях и задержках, регистрируемых в информационной системе предприятия.

Обособленно стоит проблема информационных угроз при использовании различных информационных сетей. В современных условиях сеть как система децентрализованного управления приобретает все большее значение. По сетевому принципу фирмы строят свои внутренние и внешние связи[2].

С учетом того что угроза может переходить из категории "возможная" в категорию "потенциальная", необходимо оценить привлекательность реализации конкретной угрозы (возможно, класса угроз) для потенциального нарушителя.

Важным является решение вопроса об определении критериев эффективности системы информационной безопасности, к которым можно отнести: технические, социальные, экономические, эффективность управленческой деятельности.

Изучение характеристик существующих аппаратно-программных средств защиты позволяет определить, какие из имеющихся вариантов удовлетворяют всем разработанным критериям информационной безопасности. Выбираются и системы шифрования, которые будут использоваться в процессе обработки, приеме-передаче, хранении и обновлении информации в системе. Как показывает практика, чем больше возможность охватить рассматриваемые системы и чем разнообразнее применяемые методы, тем надежнее будет функционировать система информационной безопасности промышленного предприятия. Однако, решая вопрос с разнообразием применяемых технологий, методов и средств, не стоит забывать о проблеме совместимости их с уже функционирующей системой, с обязательным учетом аппаратной части, операционной системы, а также прикладных программ.

Исследовательский этап предполагает разработку политики безопасности, определение допустимой степени риска, набора процедур и методов исключения возможного несанкционированного доступа к ресурсам информационной системы предприятия и т.д. Для этого применяются специальные оценочные шкалы допустимых потерь, учитывающие потери как в натуральном, так и в денежном эквиваленте. Следует учитывать, что потребуется разнообразие оценочных шкал, так как в каждой информационной системе, подсистеме и так далее существует граница "допустимости" потерь, которая определяется ценностью хранимой информации, масштабом разработок, финансовым бюджетом, а также множеством других экономических, организационных, морально-этических, политических и прочих факторов.

В том случае, если расчетные потери меньше, чем потребные затраты на разработку, последующее внедрение и эксплуатацию средств защиты, и с позиции интересов информационной системы потенциально возможный несанкционированный доступ не должен привести к существенным сбоям и изменениям в работе, то данный риск следует считать приемлемым. При этом следует учитывать, что в большинстве случаев необходимо исключить даже незначительную утечку информации, как, например, когда идет речь о смысловом содержании конфиденциальной информации, содержащей анализ конъюнктуры рынка, перечень новых технологий, стратегий развития, планов и бюджетов.

В проведении работ исследовательского этапа наиболее ответственными являются работы, связанные со сложностью разработки и принятия политики безопасности. В общепринятом смысле под политикой безопасности понимают систему правил, законов, практических рекомендаций и процедур, которую используют как основу управления, защиты и распределения критической информации в информационной системе промышленного предприятия. Прорабатываемая политика безопасности должна будет охватывать все особенности процесса обработки информации, с большой долей вероятности определять возможное поведение системы в различных ситуациях.

Немаловажным моментом является проработка различных механизмов обнаружения попыток несанкционированного доступа к защищаемым ресурсам. Данные механизмы могут базироваться на экспертных системах. Они также должны включать распознавание, регистрацию и обработку событий, связанных с несанкционированным доступом к информации, а так-

же проводить в реальном времени проверку соответствия всех условий доступа, принятых в разработанной концепции системы информационной безопасности промышленного предприятия и защиты его данных.

В случае наступления негативных последствий несанкционированного доступа в рамках данного этапа также предусмотрена разработка плана восстановления и обеспечения нормальной работы информационной безопасности.

Следует отметить, что такие этапы, как аналитический и исследовательский, логически могут быть объединены в один общий этап, основной задачей которого является изучение рисков.

Данный момент регулируется особенностями информационной системы каждого отдельно взятого промышленного предприятия.

На основе полученного результата проработки возможных угроз будет создан комплекс контрмер и мероприятий, обеспечивающий необходимый и достаточный уровень защищенности информационной системы предприятия.

Испытательный этап по своему содержанию заключается в последовательном исследовании различных вариантов размещения всех элементов системы информационной безопасности, с последующим выбором оптимального решения, основанного на соотношении эффективность/стоимость, документировании, тестировании, оформлении итоговых рекомендаций к внедрению.

Осуществив исследование и сделав выбор по критериям эффективность/стоимость, а также комплекс работ, связанных с размещением элементов системы информационной безопасности в узлах информационной системы, проводится анализ полученных результатов. Для гарантирования устойчивости системы информационной безопасности при реализации различного рода атак проводят ее тестирование с использованием функциональных тестов. На основе отчета о тестировании может быть принято решение об использовании модулей системы информационной безопасности, а в случае получения неудовлетворительного результата - о доработке либо замене того или иного модуля. Важным шагом является расчет ожидаемого эффекта от внедрения конкретной системы информационной безопасности, на базе которого может быть принято управленческое решение об использовании либо доработке конкретной конфигурации системы информационного обеспечения промышленного предприятия.

Заключительным шагом в рамках испытательного этапа является документирование, состоящее в разработке пакета методических, инструктивных, технологических материалов, которые подробным образом описывают структуру и принципы функционирования системы информационной безопасности; способы и механизмы реализации ее возможностей, план восстановления ресурсов информационной системы в случае наступления негативных событий и т.д.

Этап внедрения и последующей технической поддержки будет включать уже непосредственно работы по вводу системы информационной безопасности в эксплуатацию с последующим обучением и аттестацией персонала. На данном этапе также предусматривается дальнейшее развитие и поддержка системы информационной безопасности на должном уровне, проведение регулярного тестирования, которое должно осуществляться на протяжении всего жизненного цикла системы информационного обеспечения предприятия с целью выявления новых видов угроз, которые не были предусмотрены при ее проектировании, разработке и внедрении.

Своевременная модификация и развитие отдельных компонентов могут осуществляться исключительно на основе полученной актуальной информации о новых угрозах и каналах утечки информации.

Изложенный процесс разработки, проектирования и внедрение системы информационной безопасности на промышленном предприятии по своей сути является инновационным проектом. Цель данного проекта - необходимость формирования на базе определенной концепции и необходимого методологического обеспечения комплексной системы защиты информационных ресурсов промышленного предприятия с использованием современных средств, новейших разработок,

отвечающих современному уровню информатизации, и требований по информационной безопасности, выполняемых за счет инвестиций в НИОКР и внедрения на коммерческой основе средств, комплексов и систем.

В процессе реализации инновационного проекта системы информационной безопасности следует уделить внимание следующим основным принципам:

♦ Применение системного подхода. Он предполагает обязательный учет следующих факторов: обеспечение защиты всех видов информационных ресурсов, процессов и видов деятельности независимо от их природы, средств и технологии, организации и средств реализации обеспечения безопасности объекта; в процессе управления безопасностью отождествление системы с типовыми рабочими проектами, в основу формирования которых положены классификации различных видов информационной деятельности или информационных ситуаций, с учетом выделения функциональных и обеспечивающих подсистем в рамках системы информационной безопасности промышленного предприятия.

♦ Обязательный учет экономической целесообразности в процессе комплектования средств. В рамках конкретного проекта средства защиты информации комплектуются из тех, что имеются в настоящий момент на рынке. При осуществлении выбора обязательно сравниваются показатели эффективности их работы, а также стоимость. При этом соотношение минимальной стоимости и эффективности определяется либо на основании исходных данных пользователя, либо путем предпроектного обследования объекта.

♦ Обоснование экономической целесообразности инвестиций. Инвестирование в создание новых средств защиты может быть практически осуществлено только после подтверждения целесообразности их осуществления. Данное экономическое обоснование выполняется с учетом исследования состояния информационных технологий, реальных потребностей и рынка средств защиты.

♦ Конструкторская полнота рабочих проектов. Рабочие проекты систем защиты информации промышленного предприятия должны включать средства, технологическую, конструкторскую и эксплуатационную документацию, которая позволит заказчику реализовать проект.

♦ Коммерческая реализация всех разделов рабочих проектов. Имеет смысл предусмотреть возможность реализации рабочих проектов по разделам, подсистемам, модулям системы информационной безопасности. В данном случае набор средств следует ориентировать на решение задач защиты определенной информационной деятельности промышленного предприятия или для обеспечения максимально уязвимых информационных процессов и ситуаций.

♦ Поэтапная реализация инвестиционного проекта. Для получения максимальной эффективности от проекта необходимы первоначальные ресурсные вложения с последующим наращиванием сферы и объемов деятельности в зависимости от реакции на данные усовершенствования.

В процессе реализации инновационного проекта следует решить ряд задач методического плана:

1. Разработать и утвердить концептуальные положения защиты информационных ресурсов промышленного предприятия.

2. Создать методическое обеспечение для проведения обследования объектов и дальнейшего принятия решений в области их комплексной защиты.

3. Провести классификацию средств защиты информационных ресурсов предприятия, осуществить оценку их сертификационных качеств, а также возможность дальнейшей совместимости систем.

4. Предложить типизацию всех объектов с целью создания для них универсальных вариантов рабочих проектов по защите информации в информационной среде промышленного предприятия.

5. Разработать и внедрить в процесс оценки инвестиций методическое обеспечение для подтверждения экономической целесообразности и технической возможности инвестиций в области информационной безопасности.

6. Разработать методическое обеспечение для проведения оценки информационной безопасности различных объектов промышленного предприятия.

7. Разработать технологии и принципы маркетинга и продвижения рабочих проектов и средств по защите информационных ресурсов промышленного предприятия.

В качестве практической базы реализации инновационного проекта выступают средства защиты информации, различная конструкторская и эксплуатационная документация типовых рабочих проектов системы информационной безопасности, организация и технология реализации проекта.

Одним из подходов, применяемых при оценке качества защиты информации предприятия, является определение соответствия техническому заданию на создание системы информационной безопасности, а также комплекса реализуемых функций и задач, важных эксплуатационных характеристик, предъявляемых специфических требований и многого другого.

Другим вариантом оценки выступает анализ функциональной надежности системы предприятия, которая также может рассматриваться как характеристика качественного уровня системы информационной безопасности промышленного предприятия. При этом количественный уровень защиты информационной системы предприятия характеризуется двумя основными группами показателей - относительными и абсолютными.

Относительная количественная оценка представляет собой некоторое число (рейтинг, категорию), которое будет подвергаться сравнению с другими числами, принятыми в качестве эталонного значения. Как правило, для их определения используется экспертный подход к оценке.

Важным моментом в проведении качественной оценки является вопрос о корректировке и согласовании допустимых погрешностей, которые, как следствие, возникают в связи с субъективностью оценок экспертов. Проведение экспертизы может быть направлено на следующие факторы: оценку эффективности системы защиты, оценку уровня допустимого риска, уровня защищенности отдельных подсистем и др.

В случае, когда в качестве объекта оценки выступает информационная система, считаем целесообразным разработать комплекс механизмов, который позволит получить количественные показатели защищенности системы промышленного предприятия.

Абсолютная количественная оценка защиты информации в информационной системе может быть охарактеризована размером издержек, выраженных в стоимостном выражении, либо частотой неблагоприятных событий, которые являются значимыми в части обеспечения защиты информации промышленного предприятия. Данные показатели можно систематизировать в ряд разновидностей:

♦ Экономические показатели характеризуют объемы затрат, источники, условия привлечения и порядок вложения средств в обеспечение информационной безопасности, а также определяющие экономическую эффективность вложенных средств.

♦ Технические показатели характеризуют сугубо технические аспекты процесса защиты информации, в том числе такие, как качество защиты, количество блокируемых угроз и многое другое.

♦ Организационные показатели характеризуют аспекты организации разработки, внедрения, эксплуатации и сопровождения системы информационной безопасности предприятия и связанные с этим проблемы. Данная группа показателей также характеризует влияние системы информационной безопасности на процесс управления и эффективность принятых решений.

♦ Социальные показатели характеризуют влияние системы информационной безопасности на социальные аспекты отношений в коллективе, их видоизменение и влияние на социальные процессы.

Все изложенное позволяет сделать вывод, что решение проблемы путем построения единого концептуального подхода к разработке концепции системы информационной безопасности промышленного предприятия с учетом компонентов инновационного подхода к процессу, а также необходимого экономического обеспечения информационной безопасности возможно. Наиболее актуально видится путь оптимизации структуры системы информационной безопасности промышленного предприятия с учетом эффективности и осуществляемых затрат на обеспечение информационной безопасности, проведение оценки экономической эффективности системы и технической возможности обеспечения ин-

формационной безопасности, внедрения методики выбора оптимальных вариантов решений системы информационной безопасности с экономической и технической точек зрения, оценки инвестиционной привлекательности проектов системы информационной безопасности промышленных предприятий.

Методы и средства обеспечения информационной безопасности системы необходимо разрабатывать на базе актуальных научных достижений. Для успешного управления системой информационной безопасности руководители промышленного предприятия должны использовать современные подходы разработки концепции безопасности предприятия, продолжая постоянно заботиться об актуализации базы знаний предприятия по информационной безопасности. Важно контролировать работу соответствующих служб по мониторингу новых угроз информационной безопасности и проводить оценки потенциально возможных угроз для данного конкретного промышленного предприятия. Процесс обеспечения информационной безопасности является непрерывным и не допускает приостановку в системе защиты информации предприятия, а в случае допущения ошибок возможны очень серьезные и крайне нежелательные последствия. Систему информационной безопасности предприятия необходимо рассматривать не только как систему, обеспечивающую защиту бизнеса, но и как надежного партнера в достижении устойчивого развития.

---

[1] *Королев А.А.* Выбор информационной системы управления при планировании новых производств в организации // Вестник Самарского государственного экономического университета. 2013. № 12 (110). С. 66.

[2] *Казарин С.В., Ашмарина С.И.* Информационное общество как современная среда осуществления социально-экономических процессов // Вестник Самарского государственного экономического университета. 2012. № 11 (97). С. 49.

Поступила в редакцию 27.01.2015 г.