ПРАКТИЧЕСКИЕ АСПЕКТЫ РАЗРАБОТКИ И ВНЕДРЕНИЯ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Михаил Нищий,
зксперт (Республика Молдова)

The purpose of this article is to discuss practical aspects of the development and implementation of information security policy in an organization providing social services to the population

Целью настоящей статьи является обсуждение практических аспектов разработки и внедрения системы управления информационной безопасностью в организации, предоставляющей социальные услуги населению.

Под политикой информационной безопасности в данной работе понимается: разработанный в соответствии с требованиями международных стандартов нормативный документ, определяющий правила и требования информационной безопасности, систему мер, порядок действий. Документы, разработанные для внедрения политики ИБ, должны определить: зоны ответственности сотрудников организации за информационные ресурсы, за применение требований ИБ в своих зонах ответственности, регламентацию механизмов контроля в определенной области обеспечения безопасности.

Внедрение политики ИБ предполагает разработку совокупности документированных правил, регламентов, процедур, инструкций или руководящих принципов в области информационной безопасности, которыми должны руководствоваться сотрудники организации в своей повседневной деятельности.

Одним из основных условий эффективного функционирования системы управления ИБ является вовлеченность руководства организации в процесс разработки и внедрения системы управления ИБ. При этом важно отметить необходимость понимания всеми сотрудниками организации следующих основных моментов: 1) вся деятельность по обеспечению ИБ инициирована руководством организации и обязательна для выполнения всеми сотрудниками компании, 2) руководство компании лично контролирует разработку и функционирование системы управления ИБ, 3) само руководство выполняет те же правила по обеспечению ИБ и требует того же от сотрудников организации.

Разработка политики безопасности собственными силами – длительный и трудоемкий процесс, требующего высокого профессионализма, отличного знания нормативной базы в области ин-

формационной безопасности. В соответствии с принятой практикой руководством организации было принято решение выбрать внешнюю специализированную компанию для проведения аудита информационной безопасности (ИБ) автоматизированных информационных ресурсов организации и разработки концепции и политики ИБ.

Аудит ИБ представляет собой комплекс мероприятий получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности в компании, проводимый независимыми экспертами в соответствии с бизнес-процессами компании и международными стандартами. В соответствии с поставленными целями была определена область аудита и объекты аудита. Аудит ИБ позволил установить соответствие уровня информационной безопасности организации выдвигаемым внутренним требованиям, требованиям действующего законодательства и международных стандартов.

Проведенный аудит основывался на следующих принципах: 1) применение моделей нарушителей, как внутреннего нарушителя, так и внешнего нарушителя; 2) определение области проведения аудита; 3) анализ влияния выявленных уязвимостей на защищенность всей информационной системы в целом и отдельных ее компонент; 5) поиск новых уязвимостей; 6) наличие строгой системы классификации уязвимостей.

В докладе обсуждаются некоторые практические вопросы порядка выполнения аудита системы управления ИБ организации, полученные результаты и рекомендации, представленные компанией аудитором.

По результатам материалов детального отчета и анализа, проведенного аудита системы управления ИБ и в соответствии с согласованными требованиями в области ИБ, были разработаны основные документы по ИБ, в том числе, Концепция ИБ, Политика ИБ, основные Регламенты и другие организационные и распорядительные документы .

Для внедрения процессов управления ИТ-рисками в организации был разработан Регламент управления рисками, методика инвентаризации, категорирования и оценки рисков информационных ресурсов организации.

Анализ информационных рисков – составная часть процесса управления рисками. При выполнении работ по анализу информационных рисков были оценены уязвимости информационной инфраструктуры организации к угрозам информационной безопасности, их критичность и вероятность ущерба, выработаны контрмеры по уменьшению рисков до приемлемого уровня и предложены методы контроля для защиты информационной инфраструктуры.

Оценивая информационные риски, ИТ-специалисты не ограничились только лишь одними информационными системами, программным,

аппаратным и коммуникационным обеспечением, а также были рассмотрены вопросы физической безопасности и учтены и вопросы, связанные с человеческим фактором.

Как показывает практика оценку ИТ-рисков желательно проводить не реже одного раза в год, чтобы можно было гарантировать, что не остались не выявленными новые опасности, а противодействие выявленным рискам осуществляется эффективно. Внутри организации работа по оценке рисков должна быть организована на основании разработанных и утвержденных Регламентов, процедур и инструкций и согласована с риск менеджментом бизнес процессов организации. В целях повышения эффективности и качества работ в данном направлении желательно автоматизировать процессы управления информационными рисками в организации.

Выводы:

1. Политика информационной безопасности – это организационно-правовой и технический документ одновременно. В этой связи при разработке мероприятий по внедрению и реализации политики ИБ необходимо опираться на принцип разумной достаточности и экономической целесообразности.

2. Внедрение политики ИБ требует регламентации практически всех процессов обработки, хранения, передачи и обмена информации, разработки документированных процедур и инструкций. В этой связи целесообразно использовать имеющиеся стандартные методологии для повышения качества подготавливаемых документов (например, библиотека ITIL, методология Microsoft MOF и т.д.).

3. Как показывает практика, организационные меры играют очень важную роль во внедрении мероприятий политики ИБ в организации, поэтому необходимо организовать непрерывное повышение осведомленности, повышения квалификации и обучения сотрудников организации в области ИБ. В качестве перспективного подхода, как показывает практика, является использование дистанционного обучения и E: Learning.

Список литературы:

1. ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
2. ISO/IEC 17799:2005 Информационная технология. Практические правила управления информационной безопасностью.
3. ISO/IEC 27005:2008 Информационная технология – Методы Безопасности – Управление рисками информационной безопасности.
4. Н.Куканова. Практические аспекты применения международных стандартов безопасности информационных систем. ISO 27001: 2005. http://dsec.ru.