Оксана ОСАДЧЕНКО, МЭА

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Information Security Policy of Enterprise

In this report will be examined questions about importance of document Information Security Policy (ISP) and about international standards in domain of IS. Life cycle of ISP will be examined more elaborately. The classification of information threat, of information assets and of documents is presented in the context of this question also.

Информация – это ресурс, который, как и другие важные бизнес-ресурсы, имеет определенную ценность для организации, а это значит, что она нуждается в соответствующей защите. Таким образом обеспечение информационной безопасности является необходимым условием функционирования любой компании, а создание политики безопасности – одно из первых требований к организации информационной безопасности предприятия.

Политика безопасности – документ, в котором определены концептуальные и общеорганизационные вопросы информационной безопасности, отражены основные направления, цели и задачи, обязательства и важнейшие принципы деятельности предприятия в области информационной безопасности, официально сформулированные его высшим руководством и принятые к обязательному выполнению на предприятии. Политика информационной безопасности (ПИБ) является одной из нескольких политик, которыми обычно руководствуется организация. Остальные, как правило, регулируют такие важные области, как кадровая политика, распоряжение производственными мощностями и финансовая деятельность. ПИБ должна дополнять другие политики и способствовать их выполнению. Для каждой информационной системы (ИС) ПИБ должна быть индивидуальной. Она зависит от технологии обработки информации, используемых программных и технических средств, структуры организации т.д. Необходимость разработки ПИБ объясняется необходимостью формирования основ планирования и управления информационной безопасностью (ИБ). Цели разработки ПИБ – минимизация рисков бизнеса путем защиты интересов компании в информационной сфере; планирование и поддержка непрерывности ведения бизнеса; сведение к минимуму ущерба от событий, таящих угрозу безопасности, посредством их предотвращения; обеспечение целостности и доступности информации циркулирующей в организации; обеспечение рациональной эксплуатации информационных систем и ресурсов; предотвращение утечки

конфиденциальной информации; защита от несанкционированного доступа; повышение дисциплинарного уровня сотрудников при работе с внутренними информационными системами и ресурсами и другие. Принципы разработки ПИБ заключаются в следующем: невозможность миновать защитные средства; усиление самого слабого звена; расположение наиболее важных документов в зоне максимальной безопасности; минимизация привилегий; разделение обязанностей; многоуровневая защита; разнообразие защитных средств; простота и управляемость информационной системы; обеспечение всеобщей поддержки мер безопасности.

Некоторые предприятия в качестве основы ПИБ используют международные стандарты, что значительно улучшает качество системы ИБ. Например, TCSEC (стандарт США), известный как «Оранжевая книга», стал первым признанным стандартом, который описывал критерии оценки компьютерных систем. В этом стандарте впервые упоминаются такие важные понятия, как *безопасная система, политика безопасности, уровень гарантированности, монитор обращений, периметр безопасности и другие понятия.* Другой стандарт – BS 7799 (британский стандарт), первая часть которого называется «*Управление информационной безопасностью»*. Использование этого стандарта позволяет коллективно использовать информационные активы (ИА), одновременно обеспечивая их защиту. В этом стандарте выделено 10 групп регуляторов безопасности в т.ч. и политика безопасности. Еще один стандарт ISO/IEC 17799:2000 в основе которого лежит рассмотренный выше стандарт BS 7799. По составу и структуре эти два стандарта очень схожи. Кроме описанных стандартов существуют и другие: FIPS 140-2, ISO 9001, ISO 15408, COBIT, ITIL.

Обобщая информацию, полученную из различных стандартов можно выделить 5 основных этапов Жизненного Цикла (ЖЦ) разработки документа ПИБ. Первый этап – это *Аудит* существующей системы ИБ. Аудит - это процесс, с которого начинаются любые планомерные действия по обеспечению ИБ в организации. Он включает в себя проведение обследования, идентификацию угроз, ресурсов, нуждающихся в защите и оценку рисков. Таким образом – цель аудита - анализ текущего состояния ИБ и выявление всех существующих уязвимостей. В результате проведения аудита, создается список замечаний, а также рекомендаций по их исправлению. В рамках аудита проводится полная инвентаризация существующих ИА предприятия и их анализ. Второй этап ЖЦ ПИБ – *Разработка ПИБ*. На основании результатов аудита определяются основные условия, требования и базовая система мер по обеспечению ИБ в организации. Эти меры (иначе говоря – правила) оформляются в виде согласованных в рамках рабочей группы решений и утверждаются руководством организации. Однако для их написания необходимо

определиться с пятью основными вопросами: 1. Что защищать? Защищать надо ИА предприятия. *Информационный актив* – это любое оборудование, процесс или данные, связанные с информацией и подлежащие защите. Составные части ИА: технические средства автоматизации – компьютерное оборудование и средства связи; прикладное и системное программное обеспечение; электронные носители информации всех видов; информация в виде файлов и баз данных на электронных носителях; работники предприятия. 2. От чего защищать? Защищать необходимо от различных угроз. *Угроза* – это действие или событие, которое может привести к искажению, разрушению или несанкционированному использованию ИА. Применение определенных мер защиты зависит от отношения угрозы к определенной классификационной группе. В работе предложена следующая система классификации: по целям возникновения; по направлениям защиты; по источникам возникновения; по способу воздействия на ИС. 3. Как защищать? *Защита* – это комплекс мероприятий производимый с целью предотвращения ущерба от действия угроз безопасности, который ведут к утечке, хищению, утрате, искажению информации. Можно выделить несколько основных методов защиты: препятствия, управление доступом, маскировка, регламентация, принуждение, побуждение. К средствам защиты относятся: технические; программные; организационные; морально этические; законодательные. 4. Ответственность. Ключевым элементом политики является доведение до каждого его обязанностей по поддержанию режима безопасности. Политика не может предусмотреть всего, однако она обязана гарантировать, что для каждого вида проблем существует ответственный. 5. Степень защиты. В зависимости от видов информации и ее классификации существуют различные степени защиты и разграничения доступа. Некоторые из них регламентируются законодательством РМ.

Третий этап ЖЦ ПИБ – *Внедрение*. Тут возникают наибольшие трудности, как правило, связанные с необходимостью решения технических, организационных и дисциплинарных проблем. Необходимо не просто довести содержание ПБ до сведения всех сотрудников организации, но также провести обучение и дать необходимые разъяснения сомневающимся, которые пытаются обойти новые правила и продолжать работать по старому. Четвертый этап - *Контроль*. Соблюдение положений ПБ должно являться обязательным для всех сотрудников организации и должно непрерывно контролироваться. Особенно важен тщательный контроль на начальном этапе внедрения. Пятый этап ЖЦ - *Пересмотр и корректировка* правил. Необходимость постоянного пересмотра правил ИБ связана с постоянно меняющейся ситуацией на рынке информационных технологий и возникновение новых видов угроз и средств защиты.

ИБ может быть обеспечена только на основе комплексного подхода, реализация которого начинается с разработки и внедрения эффективных ПИБ. Эффективные ПИБ определяют необходимый и достаточный набор требований безопасности, учитывают особенности бизнес-процессов, поддерживаются руководством, позитивно воспринимаются и исполняются сотрудниками организации, минимально влияют на производительность труда.

Литература:

1. http://www.bre.ru/security - статья Астахова А. «Разработка и внедрение эффективных политик информационной безопасности»;
2. http://www.intuit.ru – курс «Стандарты Информационной Безопасности»;
3. http://www.security.ukrnet.net – публикация Домарева В.В. «Политика информационной безопасности»