

Итак, информация -это вся совокупность сведений об окружающем нас мире, о всевозможных протекающих в нем процессах, которые могут быть восприняты живыми организмами, электронными машинами и другими информационными системами. Человечество всегда стремилось сохранить, передать и преобразовать информацию. Это послужило толчком к появлению различных изобретений, в корне изменивших жизнь.

Стремление получать достоверную информацию вовремя, быть первым во всем, зарабатывать, умело применяя свои знания, все это явилось фундаментом к становлению новых технологий, применению их в повседневной жизни. Мы облегчили свой быт, труд, отдых и сейчас просто не представляем себя без различных гаджетов, а Интернет – это неисчерпаемый источник возможностей, потенциал которого еще не до конца изучен и раскрыт.

Литература

1. Информационные технологии в экономике: учебное пособие [Текст] / Ю.Ф. Симионова. – Ростов н/Д: Феникс, 2003. – 346 с.
2. Информационные технологии в бизнесе: учебное пособие [Текст] / И.Г. Гниденко, С.А. Соколовская. – СПб.: Вектор, 2005. – 155 с.
3. Информационные технологии в менеджменте: учебное пособие для студентов бакалавров, магистров вузов, обучающихся по направлению подготовки 080200 «Менеджмент» [Текст] / В.И. Карпузова и др. / УМО вузов России по образованию в области производственного менеджмента. – 2-е изд.. – М.: ИНФРА-М : Вузовский учебник, 2014. – 301 с.
4. Информационные технологии в экономике: конспект лекций [Текст] / А.А. Козырев, А.П. Юдин. – СПб.: Изд-во Михайлова В.А., 2000. – 64 с.
5. Информационныетехнологииивбизнесе = TheIEVMHandbookofInformationTechnolo-gyinBusiness: энциклопедия [Текст] / М. Желены ; пер. сангл.:А. Железниченко, И. Ключева, А. Ларичеваидр.. – СПб.: Питер, 2002. – 1117 с.

УДК 338

РАЗРАБОТКА СТРАТЕГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ

аспирант, Юнкерова Ю.И.

Белгород, Россия

Белгородский государственный национальный исследовательский университет

Аннотация: В условиях современной глобализации экономики и развитии информационных технологий вопрос информационной безопасности стоит на одном из первых мест по значимости. В данной статье рассматривается пошаговая разработка эффективной стратегии информационной безопасности, позволяющая значительно снизить информационные риски организации.

Ключевые слова: стратегия информационной безопасности, риск-менеджмент, информационные риски, управление, долгосрочное планирование.

DEVELOPING AN INFORMATION SECURITY AND RISK MANAGEMENT STRATEGY

postgraduate, Yunkerova Y.I.

Belgorod, Russia

Belgorod State National Research University

Abstract: In modern globalized economy and information technologies development, the question of information security is one of the most important. This article discusses the step by step development of an effective information security strategy, which can significantly reduce the risk of information organization.

Keywords: strategy of information security, risk-management, information risk management, long-term planning.

На сегодняшний день, вопрос информационной безопасности является одним из первостепенных вопросов глобальной экономики. Организации постоянно работают над разработкой стратегий управления информационной безопасностью и управления рисками, для снижения угроз безопасности и минимизации возможного ущерба [1, с.174]. С развитием экономики, задача обеспечения информации значительно усложнилась, так как стратегии безопасности должны распространяться на мобильные платформы, облачные системы и социальные экосистемы.

Важность разработки стратегии по обеспечению информационной безопасности часто упускается из виду. Стратегия безопасности служит ориентиром для определения политики безопасности, которая на дальнейших этапах разработки адаптируется под удовлетворение потребностей организации. На данный момент существует множество технологий и процедур защиты, однако для построения эффективной политики безопасности и минимизации рисков необходим стратегический подход, основанный на долгосрочных перспективах развития. Основными принципами программы обеспечения безопасности являются: управление рисками; политика, нормативы и стандарты, классификация информации; обучение персонала и коммуникации.

Разработка стратегии безопасности осуществляется в несколько шагов:

1. Оценка стоимости активов.
2. Оценка ситуации безопасности (экспозиции).
3. Анализ информационной безопасности.
4. Планирование и разработка стратегии безопасности.
5. Стратегическое выравнивание.
6. Связи стратегии безопасности (программы по вопросам безопасности).

Рассмотрим каждый из них подробно.

Шаг первый: Оценка стоимости активов.

Первый этап включает в себя процесс определения текущего и желаемого состояния безопасности организации. Подход основан на оценке стоимости актива (при этом активом могут служить данные, системы и среды), а также на оценке затрат (времени, усилий и ресурсов, требуемых для достижения желаемого состояния безопасности организации).

Шаг второй: Оценка ситуации безопасности (экспозиции).

Оценка людей, процессов и технологий в рамках организации определение необходимых изменений для гарантии приемлемой стратегии безопасности, что определяет экспозицию. Оценка ситуации безопасности довольно сложный и трудоемкий процесс, для ее осуществления необходимо собрать информацию о безопасности как внутри организации так и от внешних источников [5, с.224]. Для чего необходимо оценить следующие аспекты организации: услуги и технологии, которые поддерживают безопасность организации, техническую архитектуру, необходимую для поддержания услуг в долгосрочной перспективе, разработку нормативных актов и стандартов, а также роли и обязанности в рамках организации.

Шаг третий: Анализ информационной безопасности.

Анализ информационной безопасности проводится с целью выявления пробелов в существующей системе безопасности, определении пробелов и недочетов, нуждающихся в улучшении или корректировки, а также определение необходимых ресурсов, требуемых для достижения конечной цели безопасности. Что можно обеспечить с помощью создания структуры безопасности, состоящей из нескольких уровней: функций безопасности; безопасности мероприятий, необходимых для реализации каждой и возможностей безопасности, связанной с охранной деятельностью. Для эффективного анализа информационной безопасности необходимо рассматривать информацию с разных точек зрения.

Шаг четвертый: Планирование и разработка стратегии безопасности.

Этот шаг состоит в принятии полученной информации (в ходе сбора и анализа данных, полученных в ходе предыдущих этапов) и превращении ее в реальную и прагматичную, сбалансированную стратегию безопасности. Для этого необходимо полученные данные наложить на долгосрочный план и определить основные векторы развития.

Для того, чтобы стратегия безопасности была эффективной, она должна соответствовать следующим условиям: быть краткой, четкой и понятной; стратегия должна быть реалистичной в отношении к имеющимся ресурсам и финансированию; стратегия должна быть логически выстроена документально; стратегия должна быть гибкой (для последующей адаптации, в случае необходимости) [3, с.384].

Шаг пятый: Стратегическое выравнивание.

Цель тщательно спланированной стратегии безопасности в том, что она может постоянно развиваться и подстраиваться под изменения к окружающей информационной среде, что обеспечивает ее гибкость и адаптируемость, то есть делает ее устойчивой к внешним изменениям. Для этого необходимо создавать определенный шаблон шагов, позволяющий рассматривать различные варианты развития событий, это значит, что программа обеспечения безопасности должна иметь постоянный жизненный цикл, который можно корректировать и адаптировать под различные внешние изменения.

Жизненный цикл стратегии безопасности должен включать в себя следующие этапы: планирование и организацию; реализацию; эксплуатацию и техническое обслуживание; мониторинг, управление и оценку. Без создания такого жизненного цикла невозможно долгосрочное планирование стратегии информационной безопасности [4, с.72-76].

Стратегия безопасности должна быть функциональной на всех уровнях организации, а также должна пересматриваться как минимум один раз в год и является гибким документом.

Шаг шестой: Связи стратегии безопасности (программы по вопросам безопасности).

Для эффективного управления информационными рисками важно, чтобы внутри компании, на всех уровнях организации, понималась важность стратегии безопасности и ее влияние на процессы, активы, данные, людей внутри организации и за ее пределами (клиенты и т.д.) [2, с.107-113]. Каждый человек должен быть в курсе вопросов и проблем, стоящих перед программой безопасности и стратегия должна поддерживаться на всех уровнях управления.

Программа по вопросам безопасности, как правило, направлена на три типа аудитории: руководители, сотрудники и технические работники. Каждая форма общения, или учебного материала, или сессии должна быть адаптирована к типу аудитории, и должна раскрывать ответственность, ожидания и обязательства по каждой аудитории. Только такой подход даст возможность построения эффективной стратегии информационной безопасности.

Информационная безопасность является непрерывным процессом, требующим постоянного мониторинга и управления. Только разработка гибкой, адаптируемой под изменения среды стратегии информационной безопасности может значительно снизить информационные риски организации и привести к эффективному управлению.

Литература

1. Дубров А.М. Лагоша Б.А., Хрусталева Е. Ю. Моделирование рискованных ситуаций в экономике и бизнесе: учебное пособие. – М.: Финансы и статистика, 1999. – 174 с.
2. Завгородний В.И. Информация и экономическая безопасность предприятия. // Прикладная информатика. № 2, 2006. С. 107 –113.
3. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. – М.: АйТи-Пресс, 2004. – 384 с.
4. Симонов С.В. Методология анализа рисков в информационных системах // Защита информации. Конфидент. 2001. № 1. С. 72-76.
5. Шумский А.А., Системный анализ в защите информации / А.А. Шумский, А.А. Шелупанов. – М.: Гелиос АРВ, 2008. – 224 с.