УДК 004.056:65.012

АНАЛИЗ ЗАДАЧ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОРГАНИЗАЦИИ

А.С. Сафронов
Кандидат технических наук, доцент
Кафедра информационной безопасности
Одесский национальный политехнический университет
пр. Шевченко, 1, г. Одесса, Украина, 65044
Контактный тел.: (095) 278-75-75
E-mail: AlexanderSafronov@rambler.ru

В роботі виконано аналіз задач і сформульовані вимоги до системи управління інформаційною безпекою організації. Розглянуто життєвий цикл функціонування даної системи

Ключові слова: інформаційна безпека, управління інформаційною безпекою, життєвий цикл системи управління інформаційною безпекою

В работе выполнен анализ задач и сформулированы требования к системе управления информационной безопасностью организации. Рассмотрен жизненный цикл функционирования данной системы

Ключевые слова: информационная безопасность, управление информационной безопасностью, жизненный цикл системы управления информационной безопасностью

In this work the problems and requirements for information security management system for organizations are analyzed. The life cycle of information security management system is considered

Keywords: information security, information security management, life cycle of information security management system

Введение

Деятельность большинства современных организаций происходит в условиях глобального рынка со сложной, быстро изменяющейся структурой, при наличии конкуренции, также возможны осложнения в виде экономических кризисов и политической нестабильности. Выживание, а тем более успешное развитие организаций сегодня невозможно без грамотного, компетентного управления с применением современных технологий и методов из области проектного менеджмента и информационно-телекоммуникационных технологий. В процессе развития информационной инфраструктуры важной проблемой является обеспечение информационной безопасности организации, объединяющей задачи управления, информатизации и защиты информации.

Актуальность информационной составляющей для развития государства, и, в частности, развития организаций различных типов отражена в доктрине информационной безопасности Украины [1]. Там же показано, что качество и эффективность информационной инфраструктуры является необходимым условием для эффективного управления организацией и своевременного выявления проблем.

1. Постановка проблемы

Одной из ключевых составляющих информационной инфраструктуры организации является система управления информационной безопасностью (СУИБ). В современной науке защита информации (ЗИ) является комплексом научных дисциплин, объединяющим техническую защиту информации, криптологию, ЗИ в информационно-телекоммуникационных системах и сетях, социальные и административно-правовые методы ЗИ. Поэтому СУИБ организации должна включать как технические, так и организационные составляющие.

Кроме того, согласно требованию ст. 8 Закона Украины «Про защиту информации в информационно-телекоммуникационных системах», особые категории информации, требующие защиты (конфиденциальная, для служебного пользования, секретная) должны обрабатываться с применением сертифицированной комплексной системы защиты информации, создание и развитие которой входит в рамки СУИБ.

Научной проблемой, вызывающей необходимость исследований, является отсутствие общепринятой и эффективной методологии создания, развития систе-

мы управления информационной безопасностью организаций. Осложняющим фактором является то, что СУИБ часто необходимо создавать на фоне постоянно изменяющейся информационной структуры организации и организационных перестроек.

2. Анализ последних исследований и публикаций

Систематизированное изложение большинства вопросов информационной безопасности представлено в [2]. Отдельные направления, такие как технические средства радиообнаружения и биометрии, криптография, защита информации в компьютерных системах и сетях находятся в постоянном развитии, не отставая от общего развития информационно-телекоммуникационных технологий. К сожалению, в доступной литературе весьма редки публикации, посвященные вопросам управления информационной безопасностью, реализации проектов и методик принятия управленческих решений в данной области. Так можно выделить работы А.В. Потия, Д.Ю. Пилипенко, В.Я. Певнева, М.В. Цуранова [3,4]. В данных работах содержатся описание математических моделей процессов информационной безопасности и предложены различные показатели для оценки ИБ.

Следует отметить международные стандарты информационной безопасности: ISO/IEC 17799:2005 - «Информационные технологии - Технологии безопасности - Практические правила менеджмента информационной безопасности» и ISO/IEC 27001:2005 - «Информационные технологии - Методы обеспечения безопасности - Системы управления информационной безопасностью - Требования», но данные стандарты не достаточно полно соответствуют украинской системе законодательства в области защиты информации и зрелости украинских организаций в сфере информатизации.

Автором данной статьи в предыдущих работах рассматривались некоторые аспекты создания и управления СУИБ для украинских организаций на основе методов проектного управления [5-8].

3. Формирование целей статьи

Целью статьи является анализ требований к системе управления информационной безопасностью для современных украинских организаций при соответствии условиям законности, эффективности и экономичности. Данный анализ необходим для выявления основных требований и ограничений, которые впоследствии определят долгосрочную стратегию создания и развития СУИБ для организации.

4. Изложение основного материала статьи

Создание и развитие СУИБ является долгосрочной деятельностью, поэтому жизненный цикл СУИБ планируется на весь период стратегии развития предприятия.

Цель СУИБ состоит в обеспечении необходимого уровня и совершенствование информационной безопасности организации при соответствии условиям законности, эффективности и экономичности. Условия эффективности и экономичности индивидуальны для каждой конкретной организации.

Анализируя пожелания руководителей различного уровня и опыт построения СУИБ различного уровня можно выделить следующие требования и ограничения к СУИБ, общие для всех типов организаций:

- Как правило, СУИБ формируется для поддержки существующих информационной и организационной структур организации и поэтому «подстраивается» по конкретную организацию. В редких случаях возникает необходимость реорганизации указанных структур, что значительно удорожает СУИБ.
- Негативное влияние СУИБ на бизнес-процессы организации должно быть незначительным либо отсутствовать вообще.
- Расходы на создание и развитие СУИБ не должны оказывать значительного замедления на развитие самой организации.
- Стратегия развития СУИБ должна быть частью стратегии развития информационной инфраструктуры организации и все проекты по СУИБ должны согласовываться с проектами информатизации.
- Деятельность СУИБ является смешанной, частично проектной, частично операционной. Причем проекты являются взаимосвязанными, формируя общую программу.

С учетом типовых приоритетов и задач организаций [9] предлагается установить следующую приоритетность задачам СУИБ (в порядке убывания значимости):

- соответствие действующему законодательству и нормативным актам;
- соответствие установленному уровню расходов;
- минимизация рисков информационной безопасности;
- соответствие задачам стратегического развития СУИБ;
- минимизация негативного влияния на бизнес-процессы;
- соответствие международным стандартам ИБ.

Организовывать и поддерживать функционирование СУИБ должна отдельная структура организации. Причем нежелательно подчинять структуру ИТ департаменту организации, т.к. деятельность СУИБ будет часто вступать в конфликт с задачами и пожеланиями ИТ департамента, что в конечном итоге ухудшит эффективность СУИБ. Главная причина конфликтов - противоположные приоритеты данных структур: безопасность ухудшает скорость и удобство работы.

Процесс создания системы управления информационной безопасностью организации (СУИБ) состоит из следующих этапов:

- Осознание необходимости и принятие решения о создании СУИБ на уровне высшего руководства организации.
- Принятие решения об организации структуры/отдела СУИБ и назначение компетентного руководителя. Утверждение его полномочий и зон ответственности.

• Изучение проблематики защиты информации в организации;

• Разработка стратегии развития СУИБ.

• Создание необходимых условий для работы СУИБ: организационные решения, найм специалистов и вспомогательного персонала, материальное обеспечение.

• Оперативное планирование деятельности СУИБ на начальный период.

• Старт проектов и других мероприятий по информационной безопасности.

Учитывая данные этапы, жизненный цикл системы управления информационной безопасностью организации можно представить как совокупность проектов и операционной деятельности (рис. 1).

Первоначально для построения СУИБ в организации создаются служба или нескольких служб, выполняющих в основном контролирующие и мониторинговые функции. Важной задачей является правильное распределение прав и полномочий данной структуры. С одной стороны, должны быть достаточные полномочия для получения актуальной и объективной информации об уровне информационной безопасности (ИБ) в организации, для своевременной реакции на угрозы, но в то же время, данная контролирующая и регулирующая деятельность не должна препятствовать нормальной работе других структур организации. Другими задачами службы СУИБ является анализ рисков информационной безопасности, оценка изменений окружения и управление развитием СУИБ.

После создания базовой структуры СУИБ начинается итеративный процесс функционирования со следующими фазами:

• Анализ текущего состояния ИБ организации.

• Планирование мероприятий

• Реализация мероприятий

• Контроль эффективности

Главной особенностью жизнедеятельности СУИБ является итеративное повторение фаз развития системы, выражающихся в модернизации и совершенствовании системы, и фаз проверок, необходимых для оценки эффективности и достаточности системы на фоне непрекращающегося процесса планирования деятельности. Таким образом, можно выделить минимум три проекта в деятельности СУИБ: проект запуска, проект проверки и проект развития/модернизации.

И хотя процессы проверки и развития СУИБ являются повторяющимися, их нельзя считать только функциональной деятельностью. Результаты этих процессов всегда являются уникальными - изменяются внешние условия, изменяется структура организации, внедряются новые технологии, все это значительно влияет на информационную структуру организации и, в частности, на информационную безопасность. Большинство отдельных мероприятий по ИБ в процессах проверки и развития имеют четко выраженные сроки начала и окончания. Сам же жизненный цикл системы ИБ имеет начало, но является продолжающимся, т.к. управление информационной безопасностью - непрерывный процесс. Как правило, данные мероприятия способствуют повышению ценности информационной инфраструктуры организации.

Особым случаем является процесс аварийного устранения реализованной угрозы информационной безопасности. При этом создается новый, высокоприоритетный проект организации, который охватывает не только СУИБ, но и все необходимые ресурсы организации, даже в ущерб ее основной деятельности.

Рис. 1. Жизненный цикл системы управления информационной безопасностью организации

И хотя подобное невозможно достоверно предсказать, можно заранее спланировать адекватные меры противодействия, значительно снижающие общий ущерб.

Управление ИБ организации должно осуществляться соответствующей структурой организации со штатом своих сотрудников, при этом возможно привлечение специалистов из других структурных подразделений или даже внешних субподрядчиков, например для экспертизы или сертификации. Главная роль в управлении ИБ должна принадлежать исключительно собственным сотрудникам, поручение этой задачи внешним исполнителям является неоправданным и рискованным. Руководитель должен одновременно обладать и управленческими и специальными знаниями и навыками.

Анализируя задачи обеспечения информационной безопасности, можно сделать вывод, что наиболее эффективной формой решения является создание специализированной структуры с постоянной командой специалистов.

Наиболее предпочтительной является проектно-ориентированная форма деятельности при наличии стратегического планирования. В этом случае достигается максимальная эффективность деятельности, минимизируются риски, а также значительно повышается скорость реагирования на реализованные угрозы информационной безопасности. Наивысшими приоритетами деятельности является минимизация рисков ИБ при условии строгого соблюдения требований законодательства и минимально необходимого финансирования.

Литература

1. Доктрина інформаційної безпеки. України ЗАТВЕРДЖЕНО Указом Президента України від 8 липня 2009 року N 514/2009 [Электронный ресурс]. - Режим доступа к док.: http://www.president.gov.ua/documents/9570.html.
2. Домарев В.В. Безопасность информационных технологий. Системный подход: - К.: ООО «ТИД «ДС», 2004. - 992 с.
3. Потий А.В., Пилипенко Д.Ю. Классификация показателей безопасности информации. Системи обробки информации. Выпуск 3(84), 2010, с. 53-56.
4. Певнев В.Я., Цуранов М.В. Математическая модель информационной безопасности. Системи обробки информации. Выпуск 3(84), 2010, с. 52-64.
5. Сафронов А.С., Венедиктов Ю.И., Барабанов Н.А. Жизненный цикл системы управления информационной безопасностью организации // Труды V МНПК «Управление проектами в развитии общества», Киев, 2008. - С. 185 - 187.
6. Сафронов А.С. Проектно-ориентированное управление информационной безопасностью организации // Східно-Європейський журнал передових технологій 1/3 (43), 2010, Харьків, С. 37–38.
7. Сафронов А.С., Венедиктов Ю.И., Барабанов Н.А. Ценность информационной безопасности организации // Тези доповідей VII міжнародної конференції «Управління проектами у розвитку суспільства». Тема: Управління цінністю проектів та програм розвитку організацій, Київ, 2010. - С. 180-182.
8. Сафронов А.С., Венедиктов Ю.И., Барабанов Н.А. Риск-ориентированное управление информационной безопасностью организаций // Труды XI МНПК «Современные информационные и электронные технологии», Одесса, 24 - 28 мая 2010г. - С. 92.
9. Архитектура и стратегия информационной безопасности Cisco. Информационный бюллетень. Cisco Systems, Inc, 2009 г. [Электронный ресурс] - Режим доступа к док.: http://www.cisco.com/web/RU/downloads/Cisco_Security_Architecture.pdf.