УДК 65.012.27: 004.056.5

АНАЛИЗ ПРОЦЕССОВ РАЗВИТИЯ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

К. т. н. А. С. Сафронов, Н. А. Барабанов, Ю. И. Венедиктов

Одесский национальный политехнический университет
Украина, г. Одесса
AlexanderSafronov@rambler.ru

В работе рассматриваются процессы развития систем информационной безопасности организаций. Проведен анализ данных процессов, выявлены их основные этапы, характеристики и взаимосвязь. Сформулированы общие требования к системам информационной безопасности. Разработана общая стратегия развития данных систем. Предложен метод оценки эффективности системы ИБ.

Ключевые слова: управление информационной безопасностью, проекты и операционная деятельность организации.

Согласно действующим нормативно-правовым требованиям Украины, отечественные организации должны обеспечить безопасность информации при обработке персональных данных и конфиденциальной информации в своих автоматизированных системах [1, 2]. Для решения данной задачи в организациях, как правило, выполняется построение комплексной системы информационной безопасности (ИБ), включающей в себя как технические, так и организационные компоненты. Актуальность создания системы ИБ обусловлена возможным ущербом для организации от реализации угроз информационной безопасности, вызываемых деятельностью недобросовестных конкурентов, нелояльных сотрудников и другими внешними и внутренними факторами.

Проблемой, вызывающей необходимость исследований, является то, что при создании таких систем существует противоречие: с одной стороны необходимо минимизировать ущерб для предприятия от угроз ИБ, с другой стороны создание и поддержка системы ИБ требует постоянного расхода ресурсов организации. Также внесение процедур ИБ в бизнес-процессы может привести к их удорожанию и/или замедлению. Еще одним усложняющим фактором при построении систем ИБ является выполнение требований законодательства Украины, которые являются достаточно сложными и дорогими в соблюдении, а также изменчивыми, что в будущем потребует модернизации системы ИБ.

Таким образом, задача создания и развития эффективной системы ИБ является нетривиальной в связи с охватом всех бизнес-процессов в масштабе организации и динамичности среды функционирования, выражаемой в изменении требований законодательства, развитием информационных технологий, развитием самой организации и появлении новых угроз ИБ.

На текущий момент отсутствует единая методология построения и развития системы ИБ организации с учетом особенностей бизнеса конкретной организации, а также экономических, технических, нормативно-правовых и социальных факторов. Существующие подходы, как правило, описывают желаемый результат, метод или технологию без указания способа их достижения или внедрения [3, 4].

Целью данных исследований является анализ процессов организации ИБ и разработка стратегии построения системы ИБ, ориентированной на создание и непрерывное развитие с учетом указанной проблематики.

Первым этапом разработки системы ИБ является формулировка требований и оценка их приоритетности [5]. Так, можно выделить следующие требования:

— обеспечение доступности и нормального функционирования информационных ресурсов и служб организации для легитимных пользователей;

— минимизация вероятности реализации угроз ИБ и ущерба от них;

— выполнение требований законодательства в области защиты информации;

— реализуемость проектов построения и развития системы ИБ для возможностей организации;

— формирование самостоятельного структурного подразделения организации для решения

проблем ИБ и предоставление ему необходимых властных полномочий и ресурсов;

— минимизация негативного влияния операций по защите информации на эффективность бизнес-процессов организации;

— обеспечение возможности оценки эффективности системы ИБ для конкретной организации.

Далее, с учетом приоритета требований и возможностей организации разрабатывается стратегия развития системы ИБ, в которой формулируются общие цели и задачи защиты информации, пути их достижения, а также выбираются общие критерии и методы оценки достижения данных целей.

Второй этап построения системы ИБ — создание организационно-структурного компонента системы ИБ, обычно в виде отдельного подразделения — службы ИБ, которое подчиняется непосредственно первому лицу организации и которое является фундаментом для дальнейшего развития системы ИБ. Дальнейшие этапы развития системы ИБ проводятся уже самой службой ИБ.

После создания службы ИБ начинается третий, итеративный этап развития системы ИБ — это процессы развития системы ИБ и процессы обеспечения защиты информации. Основной проблемой данного этапа является распределение ресурсов между данными процессами. Противоречие состоит в том, что эффективность обеспечения ИБ пропорционально уровню развития системы, но затраты на развитие конкурируют с ресурсами на мероприятия по непосредственной защите информации.

Предлагается следующая стратегия развития системы ИБ, ориентированная на согласованное развитие службы ИБ и повышение уровня ИБ (см. рисунок).

Стратегия развития системы информационной безопасности

Защита информации в организации — это непрерывная деятельность, состоящая из ряда процессов, таких как анализ состояния ИБ, развитие системы ИБ, управление рисками, реагирование на инциденты, проведение плановых мероприятий и т. д. Служба ИБ обеспечивает защиту информации путем выполнения указанных процессов как совокупности взаимосвязанных проектов и операционной деятельности [6, 7].

Среди проектной деятельности службы ИБ можно выделить проекты-модули, результатом которых является непосредственное изменение уровня ИБ организации, и проекты-платформы, не влияющие напрямую на состояние ИБ, но необходимые для запуска и поддержки проектов-модулей, функциональных процессов, а также для выполнения совместных проектов организации, в которых служба ИБ выполняет консультативные и контролирующие функции.

Одним из ключевых показателей системы ИБ является ее эффективность. В работе предлагается метод оценки эффективности, основанный на стоимости угрозы ИБ. Пусть существует некоторое конечное множество угроз информационной безопасности $T \in \{T_1, T_2, \ldots, T_N\}$ размером *N*. Каждая угроза T_i, $i \in 1 \ldots N$, характеризуется двумя основными параметрами: вероятностью возникновения p_i и ущербом d_i. Тогда стоимость отдельной угрозы определяется как $V_{T_i} = p_i \times d_i$ или $V_i = p_i \times d_i$.

Для всего множества угроз общая стоимость определяется как $V_T = \sum_{i=1}^{N} p_i \times d_i$.

В результате функционирования построенной системы ИБ происходит изменение параметров угроз ИБ, как правило, в меньшую сторону. Пусть p'_i и d'_i — новые параметры угрозы T'_i, а $V'_T = \sum_{i=1}^{N} p'_i \times d'_i$ — новая общая стоимость угроз ИБ.

Оценка эффективности системы ИБ определяется как $E = \frac{\sum_{i=1}^{N} p_i \times d_i - \sum_{i=1}^{N} p'_i \times d'_i}{C_{ISS}}$ (1),

где C_{ISS} — стоимость создания системы ИБ. Другими словами, формула (1) показывает, во сколько раз общий ущерб от угроз ИБ больше затрат на создание системы ИБ.

Также необходимо учесть стоимость анализа (аудита) состояния ИБ, который выполняется до и после создания системы ИБ, тогда формула (1) примет вид $E = \frac{\sum_{i=1}^{N} p_i \times d_i - \sum_{i=1}^{N} p'_i \times d'_i}{C_{A1} + C_{ISS} + C_{A2}}$ (2),

где C_{A1} и C_{A2} — стоимости первичного анализа ИБ и анализа после построения системы ИБ.

В результате проведенного анализа процессов развития систем ИБ организаций выявлены основные проблемы построения систем такого типа, определены основные требования к ним, а также предложена общая стратегия развития системы ИБ. Сделан вывод о том, что деятельность по обеспечению ИБ представляет собой совокупность взаимосвязанных мероприятий проектного и операционного характера. Впервые предложен метод оценки эффективности систем ИБ, основанный на изменении ожидаемого ущерба от угроз после выполнения мероприятий по защите информации.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Про захист персональних даних. Верховна Рада України; Закон від 01.06.2010 № 2297-VI [Електронний ресурс: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2297-17. — 2011

2. Доктрина інформаційної безпеки України — затв. Указом Президента України від 8 лип. 2009 р. № 514/2009 [Електронний ресурс]: —http://www.president.gov.ua/documents/9570.html. — 2011

3. Сафронов О. С., Плачінда О.Є., Венедиктов Ю.І. Застосування організаційно-технічних методів для розвитку системи інформаційної безпеки організації // Праці Одеського політехн. ун-ту.– Одеса : ОНПУ.— 2011. – Вип. 1(35). – С. 262 -266.

4. Домарев В.В. Безопасность информационных технологий. Системный поход — Киев: ТИД ДС, 2004.

5. Сафронов, А. С., Венедиктов Ю.И., Барабанов Н.А. Жизненный цикл системы управления информационной безопасностью организации // Тези доп. V Міжнар. конф. «Управління проектами у розвитку суспільства».— Україна, м. Київ: КНУБА, 2008. — С. 186–189.

6. Сафронов, А. С., Венедиктов Ю.И., Барабанов Н.А., Риск-ориентированное управление информационной безопасностью организаций // Тр. XI МНПК «Современные информационные и электронные технологии», Украина, г. Одесса.— 2010. — С. 92.

7. Сафронов А. С., Проектно-ориентированное управление информационной безопасностью организации // Східн.-Європ. журн. передових технологій, Харьків: Технологический центр. —2010. — Вип. 1/3 (43) — С. 37 — 38.

A. S. Safronov, N. A. Barabanov, Yu. I. Venediktov

Analysis of the development processes for enterprise information security systems.

The authors consider the development process for enterprise information security systems. The analysis of these processes is conducted, their main stages, characteristics and correlation are identified. The general requirements for information security are determined. A general strategy for the development of these systems is proposed. A method of effectiveness evaluation of information security systems is developed.

Keywords: i*nformation security management, projects and operational activities of the organization.*