УДК 65.012.8

А.С. Сафронов, канд. техн. наук,
О.Е. Плачинда, канд. техн. наук,
Ю.И. Венедиктов, инженер,
Одес. нац. политехн. ун-т

ПРИМЕНЕНИЕ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ МЕТОДОВ ДЛЯ РАЗВИТИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

О.С. Сафронов, О.Є. Плачінда, Ю.І. Венедиктов. **Застосування організаційно-технічних методів для розвитку системи інформаційної безпеки організації.** Розглянуто завдання та проблеми розвитку систем ін-формаційної безпеки організацій. Проведено аналіз процесу розвитку даних систем та виявлено його основні етапи. Запропоновано структуру служби та загальну стратегію розвитку системи інформаційної безпеки організації.

А.С. Сафронов, О.Е. Плачинда, Ю.И. Венедиктов. **Применение организационно-технических методов для развития системы информационной безопасности организации.** Рассмотрены задачи и проблемы развития систем информационной безопасности организаций. Проведен анализ процесса развития данных систем и выявлены его основные этапы. Предложены структура службы и общая стратегия развития системы информационной безопасности организации.

A.S. Safronov, O.E. Plachinda, Yu.I. Venediktov. **Application of organizational and technical methods for enterprise's information security system development.** The tasks and problems of developing the enterprises information security systems are considered. The analysis of the development process of these systems has been carried out and its main stages are identified. The structure of service and overall development strategy of enterprise information security system has been proposed.

Актуальной задачей для отечественных организаций является обеспечение информационной безопасности (ИБ) своих рабочих процессов и информационных ресурсов, что обусловлено не только стремлением защитить свои бизнес-процессы и минимизировать риски финансовых потерь, но и современными требованиями законодательства Украины [1, 2]. Под ИБ организации подразумевается интегрированная оценка уровня защищенности совокупности ее процессов и объектов — данных на любых носителях, информационных ресурсов и сервисов, автоматизированных информационных систем и баз данных от намеренных попыток реализовать угрозу ИБ. Основные типы угроз ИБ: незаконное получение конфиденциальной информации или доступа к автоматизированной системе, уничтожение информационного ресурса или канала доступа к нему, фальсификация или модификация сообщения или информационного ресурса. Обеспечение ИБ отдельного объекта обеспечивается либо полным устранением возможности угроз, либо выполнением работ, направленных на уменьшение вероятности реализации угрозы и ущерба, причиненного реализацией угрозы.

ИБ организации считается достигнутой, если для всех информационных объектов и процессов организации достигнуты приемлемые значения уровня защищенности: риск угрозы допустим, деятельность организации не нарушает требования законодательства по ИБ, выполняются регулярные мероприятия по оценке и уменьшению рисков угроз ИБ, в случае реализации угрозы ИБ организация может оперативно восстановить свою деятельность.

Существуют следующие методы обеспечения ИБ:

— законодательные;

— организационно-технические;

— административные;

— физические (ограничение физического доступа);

— технические;

— криптография и стеганография.

Большинство организаций Украины не в состоянии самостоятельно и за приемлемую стоимость достичь и поддерживать необходимый уровень ИБ по следующим причинам:

— отсутствует должное понимание необходимости обеспечения ИБ у высшего руководства организации;

— руководством не выбраны исполнители, либо назначенные работники в силу различных причин (недостаточные полномочия, нехватка времени, противоречия с основными служебными обязанностями и др.) не в состоянии выполнять данную работу;

— нечетко сформулирована цель обеспечения ИБ или различается понимание цели у руководства и исполнителей, не выявлены в полной мере все необходимые требования к результату обеспечения ИБ организации;

— исполнители недостаточно компетентны для решения данной задачи;

— организация не в состоянии выделить необходимые средства и ресурсы.

Эти причины в публикациях по ИБ освещены недостаточно полно, а в литературе по управлению проектами рассматривались неоднократно, т.к. типичны для большинства проектов развития организаций, и задача обеспечения ИБ организации может быть представлена как задача реализации программы проектов в области защиты информации [3].

Для обеспечения ИБ общепринятым является системный подход, при котором ИБ организации рассматривается как система — объединенное множество составляющих структурных элементов вместе с зависимостями и связями между ними [4].

Характерные особенности данной системы — внешние условия ее работы интенсивно меняются и с трудом поддаются формализации, т.к. изменяются требования законодательства и экономическая ситуация в регионе, а развитие науки и техники порождает новые виды угроз ИБ. Кроме того, большинство организаций постоянно развиваются, внедряя новые информационные технологии и решения, поэтому система ИБ также должна развиваться в соответствии с изменениями организации.

Предлагается повысить эффективность создания и развития системы ИБ организации путем применения организационно-технических методов на основе службы ИБ.

Обеспечение ИБ организации можно разделить на два этапа: этап создания базовой системы ИБ (СИБ), включающей только необходимые функции, и этап развития, включающий параллельные процессы функционирования и совершенствования.

В общем случае в функции СИБ организации должны входить:

— планирование, организация, координация и оперативный контроль проектов и отдельных работ, связанных с защитой информации;

— разработка методических, нормативных и распорядительных документов, действующих в рамках организации, в соответствии с которыми должны выполняться все виды работ по обеспечению ИБ;

— научно-исследовательская деятельность, направленная на разработку новых технологий и средств выявления и предотвращения возможных угроз ИБ;

— выявление и обезвреживание угроз ИБ;

— регистрация, сбор, хранение, обработка данных о событиях в организации, которые имеют отношение к безопасности информации;

— развитие и совершенствование системы ИБ, в частности, интеграция в бизнес-процессы организации, согласованная с развитием самой организации, адаптация системы ИБ к постоянно изменяющимся внешним условиям и требованиям;

— обеспечение выполнения законодательных требований и ограничений, касающихся ИБ в процессах организации, в частности, в IT-процессах;

— постоянная работа с персоналом организации для обеспечения выполнения ими требований нормативно-правовых актов, нормативных и распорядительных документов и инструкций, касающихся защиты информации;

— работа с клиентами, поставщиками, партнерами и др. внешними сторонами, участвующими в бизнес-процессах организации, для согласования требований к ИБ в совместной деятельности.

На первом этапе создания СИБ происходит выявление и определение приоритетности ее функций, актуальных для конкретной организации. Также определяется желаемая степень интеграции данной системы в основные бизнес-процессы организации и допустимый уровень ухудшения эффективности таких процессов из-за необходимости соблюдения требования ИБ. Результатом первого этапа является описание желаемых функций и формулировка требований к СИБ [5]. Обычно эти результаты образуют концепцию ИБ организации.

Второй этап построения СИБ — создание службы ИБ в виде отдельного подразделения, которое подчиняется непосредственно первому лицу организации и должно выполнять функции СИБ. На данном этапе производится планирование первой фазы деятельности службы для достижения начального уровня ИБ. Дальнейшие этапы развития СИБ проводятся самой службой ИБ.

В законодательных актах и стандартах по управлению ИБ не указаны требования к структуре, кадровому составу и компетенции службы ИБ, поэтому данные показатели зависят от конкретных задач по защите информации и индивидуальны для каждой организации с учетом ее специфики. Как правило, перечень задач и функций службы ИБ определяется размером организации, количеством защищаемых объектов, сферой деятельности, особенностями бизнес-процессов организации, актуальными требованиями по защите информации, в т.ч. и законодательными. Результирующий уровень ИБ будет определяться всем комплексом принятых организационно-технических мер, поэтому важно охватить все доступные направления защиты информации. Так, при построении СИБ дополнительно могут учитываться внутренняя культура и традиции организации, корпоративные ценности и иные этические и психологические факторы.

Предлагается структура службы ИБ, которая состоит из системы управления ИБ, являющейся частью общей системы управления организацией и взаимосвязанных процессов и подсистем ИБ, основанных на необходимых ресурсах, технологиях и сервисах организации (рис. 1).

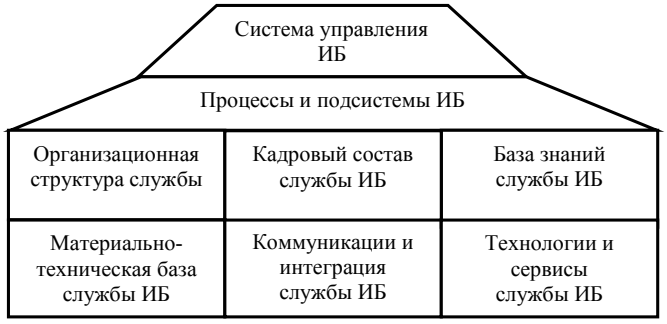

Рис. 1. Структура службы информационной безопасности организации

Организационная структура службы ИБ соответствует ее задачам и функциям, а также определяет роли, ответственность и полномочия персонала, непосредственно привлеченного к решению задач ИБ. Наиболее оптимальна матричная форма структуры, т.к. деятельность в сфере ИБ носит как проектный, так и операционный характер, а сама служба ИБ постепенно развивается.

Кадровый состав службы ИБ определяет компетенцию и возможности службы в решении задач ИБ. Можно выделить штатных сотрудников, постоянно работающих в службе, и привлеченных лиц, субподрядчиков, необходимых только на период выполнения проектов.

Материально-техническая база службы ИБ определяет совокупность технических средств, программных продуктов и необходимого оборудования для решения поставленных задач и оборудования рабочих мест для сотрудников. Организации необязательно закупать редко используемое оборудование, допустимо для отдельных работ привлекать субподрядчиков.

Технологии и сервисы службы ИБ определяют разнообразные средства автоматизации, информационные системы и подсистемы управления, такие как контроль качества, технологии проверки и тестирования, управление знаниями, аналитическое программное обеспечение, необходимые для повышения эффективности и оптимизации системы ИБ.

База знаний службы ИБ необходима для эффективного доступа к разнообразной справочной информации, накопленному ранее опыту, рабочей документации, отчетам, а также для поддержки работы автоматизированных систем.

Так как служба ИБ по своему роду деятельности должна охватывать все бизнес-процессы организации и учитывать все изменения в работе организации, важной задачей является организация и поддержка коммуникаций между службой ИБ и защищаемыми объектами. Кроме того, служба ИБ должна участвовать (хотя бы консультативно) во всех проектах, касающихся развития и совершенствования IT-инфраструктуры организации.

После создания базовой структуры службы ИБ начинается итеративный этап развития СИБ — одновременные процессы развития службы ИБ и выполнения плановых мероприятий по улучшению безопасности. Основной проблемой данного этапа является выбор приоритетов и распределение ресурсов между данными процессами. Противоречие в том, что без соответствующего развития службы ИБ ее основная деятельность будет неэффективной, и наоборот, затраты на развитие службы идут за счет экономии на мероприятиях по защите информации.

Предлагается концепция развития СИБ, ориентированная на согласованное развитие службы ИБ и повышение уровня ИБ (рис. 2).

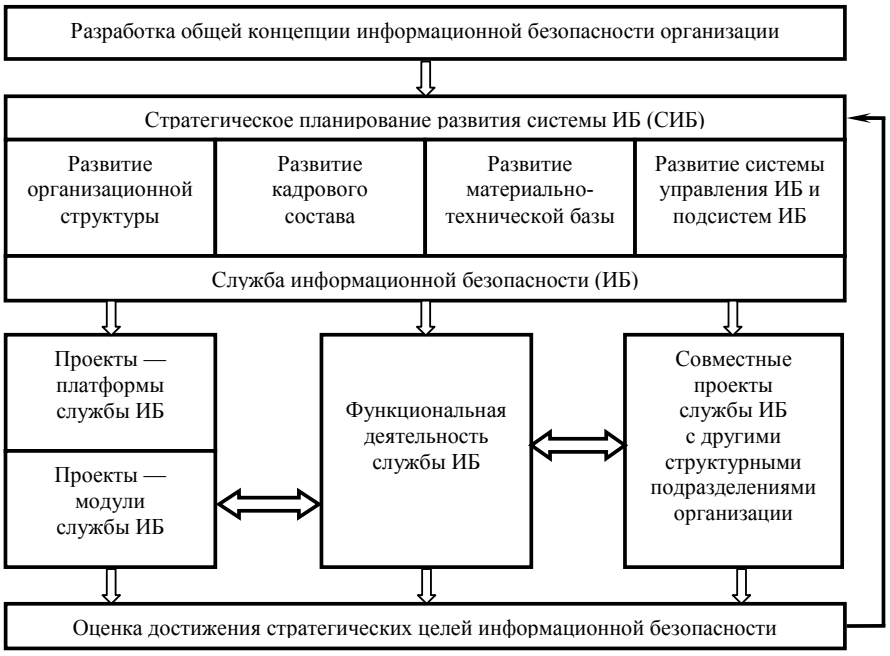

Рис. 2. Концепция развития системы информационной безопасности

Концепция развития службы ИБ является основополагающим документом, определяющим направления и приоритеты развития СИБ организации. Концепция ИБ задает цели и требования к результатам для службы ИБ, определяя структуру, материально-техническую базу и компетенцию данной службы. Далее выполняется стратегическое планирование деятельности службы ИБ на период не менее трех лет. Защита информации в организации — непрерывная деятельность, состоящая из нескольких видов функциональных процессов и одной-двух программ проектов [6, 7]. Среди проектов можно выделить проекты-модули, результатом которых является непосредственное изменение уровня ИБ организации или запуск нового функционального процесса ИБ, и проекты-платформы, не влияющие напрямую на состояние безопасности, но необходимые для запуска и поддержки проектов-модулей; а также

совместные проекты организации, в которых служба ИБ выполняет консультативные и контролирующие функции.

В результате проведенного анализа задачи обеспечения ИБ организации выявлены основные организационные проблемы построения системы ИБ, определены ее основные функции, предложена концепция ее развития. Предложен организационно-технический метод для улучшения развития СИБ на основе создания службы ИБ, представляющей собой отдельную структуру предприятия, предназначенную для решения задач защиты информации. Разработана структура службы ИБ, ориентированная на реализацию предложенной концепции развития СИБ.

Литература

1. Доктрина інформаційної безпеки України [Електронний ресурс]: Затв. Указом Президента України від 8 лип. 2009 р. № 514/2009 — http://www.president.gov.ua/documents/9570.html. — 20.03.11.
2. Про захист персональних даних [Електронний ресурс]: Закон України від 01.06.2010 № 2297-VI. — http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2297-17. — 20.03.11.
3. Ципес, Г.Л. Менеджмент проектов в практике современной компании / Г.Л. Ципес, А.С. Товб. — М.: Олимп – Бизнес, 2006. — 304 с.
4. Домарев, В.В. Безопасность информационных технологий. Системный поход / В.В. Домарев. — К.: ТИД ДС, 2004. — 992 с.
5. Сафронов, А.С. Жизненный цикл системы управления информационной безопасностью организации / А.С. Сафронов, Ю.И. Венедиктов, Н.А. Барабанов // Тези доп. V міжнар. конф. “Управління проектами у розвитку суспільства”, м. Київ, 2008р. — К.: КНУБА, 2008. — С. 186 — 189.
6. Сафронов, А.С. Риск-ориентированное управление информационной безопасностью организаций / А.С. Сафронов, Ю.И. Венедиктов, Н.А. Барабанов // Тр. XI МНПК “Соврем. информ. и электрон. технологии”, Одесса, 24 – 28 мая 2010 г. — Одесса: ОНПУ, 2010. — С. 92.
7. Сафронов, А.С. Проектно-ориентированное управление информационной безопасностью организации / А.С. Сафронов // Схід.-Європ. журн. передових технологій. — Харків: Технол. центр, 2010. — Вип. 1/3(43). — С. 37 – 38.

Рецензент д-р техн. наук, проф. Одес. нац. политехн. ун-та Гогунский В.Д.

Поступила в редакцию 11 апреля 2011 г.