ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

УДК 338.2:504.03

ЦЕЛЕВОЕ И ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ХОЗЯЙСТВУЮЩИХ СУБЪЕКТОВ

© 2016 Е. А. Жидко, К. А. Кирьянов

Воронежский государственный технический университет
ВУНЦ ВВС «ВВА» им. Н. Е. Жуковского и Ю. А. Гагарина (г. Воронеж)

В статье рассматриваются возможность создания и развития системы информационной безопасности современных хозяйствующих субъектов (компаний) и положения, которые необходимо принять за основу при разработке требований к системе информационной безопасности компании.

Ключевые слова: информационная безопасность, система информационной безопасности, конкурентоспособность.

Согласно принятой доктрине [1], информационная безопасность (ИБ) Российской Федерации рассматривается как один из главных аргументов национальной безопасности страны. Особую обеспокоенность на современном этапе вызывает ИБ отечественного производителя (т. е. хозяйствующего субъекта (ХС)), от уровня которой существенно зависит конкурентоспособность компаний и их продукции на внешних и внутренних рынках РФ. На ее подрыв направлены угрозы нарушения ИБ ХС за счет хищений, разрушения и модификации информации, которая циркулирует в системе информационных коммуникаций, необходима ей для адекватной реакции на них. Последняя должна осуществляться в интересах формирования траектории безопасного и устойчивого (антикризисного) развития ХС в реально складывающейся и прогнозируемой Геополитической обстановке [2-7].

Целевое и функциональное назначение системы ИБ ХС устанавливается, с одной стороны, исходя из требований нормативно-правовых документов по проблеме [1, 8, 9], а, с другой стороны, исходя из требований к конкурентоспособности компании, ее продукции на внешних и внутренних рынках России. [10, 11]. Поэтому при разработке требований к системе ИБ ХС целесообразно принять за основу следующие исходные положения.

Генеральная цель создания и развития СИБК, согласно требованиям доктрины [1] – поддержание баланса между: потребностью граждан, общества и государства в свободном обмене информацией; необходимыми и достаточными ограничениями на распространение информации в реально складывающейся и прогнозируемой Геополитической обстановке с учетом состязательности конкурирующих сторон, идеологической, информационно психологической и кибервойны между ними; возможности использования Геоинформационного пространства.

Путь достижения цели – оценка состояния ИБ РФ, выявление источников угроз ее нарушения, определение приоритетных направлений предотвращения, отражения и нейтрализации угроз, степень опасности последствий которых превышает допустимый уровень риска для личности, общества, государства (ЛОГ).

Главная задача СИБК на этом пути – информационная и интеллектуальная поддержка процесса формирования траектории развития компании в пределах параметров ее устойчивости в реально складывающейся и прогнозируемой обстановке.

Жидко Елена Александровна – ВГТУ, профессор кафедры пожарной и промышленной безопасности, к. т. н, доцент, e-mail: lenag66@mail.ru.
Кирьянов Константин Анатольевич – ВУНЦ ВВС «ВВА» им. Н. Е. Жуковского и Ю. А. Гагарина (г. Воронеж), ст. преподаватель кафедры управления войсками и службы штабов. Командный факультет, e-mail: konst63224@mail.ru.

Согласно требованиям [1], она должна решаться на основе:

- согласования бизнес интересов ХС с интересами ЛОГ;

- координации действий ХС в ее внешней и внутренней среде по цели, месту, времени, диапазону условий и полю проблемных ситуаций [12, 13];

- контроля результатов жизнедеятельности ХС, их экспертизы на соответствие требуемым [14, 15];

- оценки степени опасности угроз нарушения ИБ ХС, приемлемости их последствий, как для самой компании, так и для ЛОГ [16, 17];

- адекватной реакции на угрозы с неприемлемыми последствиями, в том числе на основе: предупреждения, выявления и пресечения правонарушений деятельности системы ИБ ХС в единой технической системе обеспечения ИБ РФ [2].

Программа решения главной задачи, согласно [1], базируется на современных высоких технологиях, таких как:

- моделирование и прогнозирование взаимосвязанного развития внешней и внутренней среды системы ИБ ХС; необходимости и возможности поддержания баланса между потребностями ЛОГ в обеспечении их ИБ по ситуации и результатам в статике и динамике современных условий;

- мониторинг состояний внешней среды и контроллинг состояний внутренней среды ХС;

- диагноз состояний ИБ объектов, их экспертиза на соответствие требуемым; прогноз последствий, возникающих в результате диспропорций между необходимым, потенциально возможным и реально достижимым для обеспечения ИБ ЛОГ;

- оценка приемлемости последствий нарушения ИБ ХС для ЛОГ;

- оптимизация адаптивных методов и систем защиты информации, других способов и средств обеспечения ИБ ХС по ситуации и результатам в статике и динамике;

- управленческое консультирование лиц, принимающих решение в компании, выдача рекомендаций по проектированию и программированию системы ИБ ХС, их перепроектированию и перепрограммированию по ситуации и результатам в реально складывающейся и прогнозируемой обстановке.

Реализация такой программы действий требует вполне определенного научно-методического (НМО) и научно-практического обеспечения (НПО).

В условиях состязательности конкурирующих сторон в уровне развития, идеологической, ИПВ и кибервойны между ними создание НМО и НПО, необходимого для решения главной задачи системы ИБ ХС, выливается в самостоятельную проблему. В интересах ее разрешения рекомендуется руководствоваться Политикой ИБК с учетом действующих стандартов в этой сфере [9-11].

Согласно им, «организация, в которой отсутствует Политика ИБ, похожа на государство, в котором есть полиция, но нет законов, а вместо них используются неформальные соглашения. Пойманных нарушителей нельзя обвинить, потому что формально не определено, что можно делать, а что нельзя». Здесь в качестве «аналога полиции рассматриваются методы и множество самых разнообразных систем защиты информации, при разработке которых и принятии решений на их внедрение исполнители и руководители оперируют самыми различными соображениями. Такой подход, в конечном итоге, приводит к тому, что количество и сложность методов и систем защиты информации растут, а их эффективность остается на невысоком уровне, в то время как они должны быть лишь технической основой для контроля и реализации требований, заложенных в политике ИБ ХС».

В свете сказанного «политика ИБ ХС представляет собой совокупность документов и практик, отражающих позицию и требования руководства организации и регламентирующих их деятельность по защите информации. Под совокупностью документов понимается их многоуровневая система, которая позволяет обеспечить более гибкий подход к содержанию каждого документа в зависимости от его назначения и аудитории, периодичности его пересмотра и изменения». Целевое и функциональное назначение таких документов, их основной состав и требуемое содержание на каждом уровне определяются в соответствии с принятыми стандартами.

Отсюда необходимость создания системы ИБ ХС, целевое и функциональное назначение которой определяется основными положениями всей совокупности документов в рассматриваемой сфере.

ЛИТЕРАТУРА

1. Доктрина информационной безопасности Российской Федерации: утв. Президентом РФ 9 сентября 2000 г., № Пр-1895 [Электронный ресурс].

2. Жидко Е. А. Методология исследований информационной безопасности экологически опасных и экономически важных объектов: монография. – Воронеж, 2015. - 183 с.

3. Жидко Е.А. Высокие интеллектуальные и информационные технологии интегрированного менеджмента XXI века: монография. – Воронеж, 2014. – 110 с.

4. Жидко Е. А. Методология формирования системы измерительных шкал и норм информационной безопасности объекта защиты // Вестник Иркутского государственного технического университета. – 2015. № 2 (97). – С. 17-22.

5. Жидко Е. А. Методология формирования единого алгоритма исследований информационной безопасности // Вестник Воронежского института МВД России. – 2015. – № 1. – С. 62-69.

6. Жидко Е. А. Научно-обоснованный подход к классификации угроз информационной безопасности // Информационные системы и технологии. – 2015. – № 1 (87). – С. 132-139.

7. Жидко Е. А. Логико-вероятностно-информационное моделирование информационной безопасности / Е. А. Жидко, Л. Г. Попова // Вестник Казанского государственного технического университета им. А.Н. Туполева. – 2014. – № 4. – С. 136-140.

8. Государственная информационная политика компании.

9. ГОСТ Р ИСО/МЭК 15408-1-2002 Политика безопасности организации.

10. ГОСТ Р ИСО 9000 - 2001. (Серия стандартов управления качеством).

11. ГОСТ Р ИСО 14001-98. Системы управления окружающей средой. Требования и руководство по применению. – М.: 1998. – 96 с.

12. Сазонова С. А. Методы обоснования резервов проектируемых гидравлических систем при подключении устройств пожаротушения / С. А. Сазонова // Вестник Воронежского института ГПС МЧС России. – 2015. – № 4 (17). – С. 22-26.

13. Сазонова С. А. Обеспечение безопасности гидравлических систем при реализации задач управления функционированием и развитием // Вестник Воронежского института ГПС МЧС России. – 2016. – № 1 (18). – С. 22-26.

14. Жидко Е. А. Анализ состояния атмосферы в регионе и социально-экономические последствия загрязнения окружающей среды / Е. А. Жидко, В. С. Муштенко // Высокие технологии в экологии. – Воронеж, 2008. – С. 69-74.

15. Жидко Е. А. Методический подход к идентификации экологического риска, учитываемого в деятельности предприятия / Е. А. Жидко, В. С. Муштенко // Высокие технологии. – Экология. – 2011. – № 1. – С. 11-14.

16. Сазонова С. А. Управление гидравлическимим системами при резервировании и обеспечении требуемого уровня надежности / С. А. Сазонова // Вестник Воронежского института высоких технологий. – 2016. – № 1 (16). – С. 43-45.

17. Сазонова С. А. Оценка надежности работы гидравлических систем по показателям эффективности / С. А. Сазонова // Вестник Воронежского института высоких технологий. – 2016. – № 1 (16). – С. 37-39.

18. Сазонова С. А. Оценка надежности работы сетевых объектов / С. А. Сазонова // Вестник Воронежского института высоких технологий. – 2016. – № 1 (16). – С. 40-42.

19. Зайцев А. М. Аналитическое решение задачи прогрева теплоизолированных стальных конструкций при пожарах / А. М. Зайцев// Пожаровзрывобезопасность. 2004. – Т. 13. – № 3. – С. 22-29.

20. Зайцев А. М. Прогрев строительных материалов и конструкций при реальных пожарах / А. М. Зайцев // Пожаровзрывобезопасность. – 2004. – № 4. – С. 11.

TARGET AND FUNCTIONAL PURPOSE OF THE SYSTEM OF INFORMATION SECURITY OF BUSINESS ENTITIES

© 2016 E. A. Zhidko, K. A. Kiryanov

Voronezh State Technical University
Air Force Academy named after Professor N. E. Zhukovsky and Y. A. Gagarin

The article considers the opportunity of creation and development of information security system of modern economic entities (companies) and the provisions that need to be taken as a basis for developing requirements for the information security system of the company.

Key words: information security, information system security, competitiveness.