УДК 004.492.2

ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ МАЛЫХ ПРЕДПРИЯТИЙ

Годла А.С.[1)], Губенко Н.Е.[2)]
Донецкий национальный технический университет
[1)] магистрант; [2)] к.т.н., доцент

I. Постановка проблемы

В период глобальной компьютеризации и интернетизации, который сейчас переживает современное общество, все типы предприятий становятся зависимыми от информационных систем. Это делает их уязвимыми к угрозам различного характера. Поэтому, оценивание рисков информационной безопасности предприятия и создание его собственной политики информационной безопасности должны стоять на высоких позициях в списке бизнес-приоритетов собственников.

II. Цель работы

Целью исследования является обоснование необходимости управления рисками, а также проведение анализа методов оценивания рисков для формирования политики информационной безопасности малых предприятий.

III. Риск-менеджмент как эффективный способ для анализа рисков малых предприятий

В настоящий момент корпоративные сети предприятий считаются наиболее уязвимыми с точки зрения безопасности во всей их инфраструктуре. Рассмотрим стандартную схему корпоративной сети предприятия на примере интернет-магазина (рис.1).

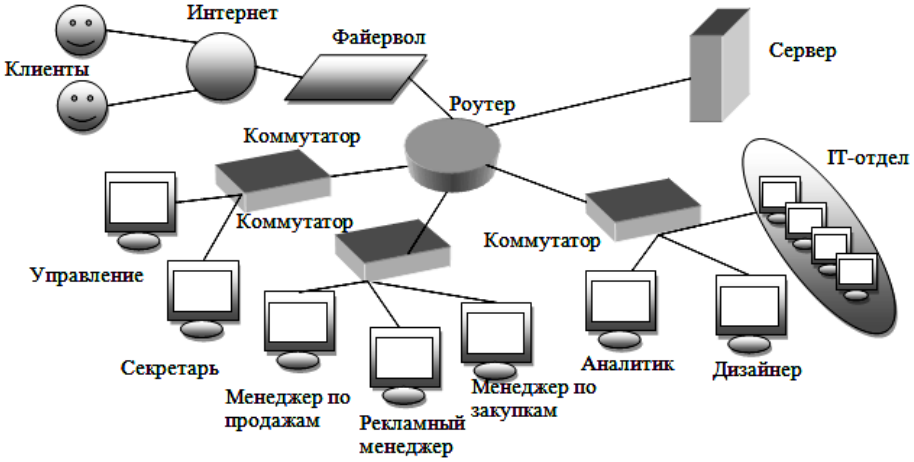

Рисунок 1 - Структурная схема малого предприятия

Как следует из ее архитектуры и методов использования, определение границ безопасности для нее практически невозможно, так как предприятие использует сеть для хранения данных, пользуется связями типа peer-to-peer, ведет переписку с помощью мгновенных сообщений, имеет удаленный доступ, а также клиентские сервисы. Поэтому, для обеспечения ИБ данного предприятия необходимо выработать некие стандартные подходы.

По словам Петренко С.А.[1], независимо от размера компании и ее конкретных информационных систем, усилия для обеспечения режима безопасности информации состоят из следующих этапов:

- определение политики информационной безопасности;
- установление границ, которые предназначены для поддержки режима информационной безопасности;
- оценка рисков;
- выбор контрмер и управления рисками;
- выбор элементов управления в целях обеспечения режима информационной безопасности;

– сертификация систем управления информационной безопасностью на соответствие стандартам безопасности.

Набор минимальных требований, к режиму информационной безопасности, перечисленных в стандартах ISO 17799 (международный стандарт), BSI (Германия), NIST 800-30 (США), составляет основу информационной безопасности. Этого набора, как правило, достаточно для целого ряда стандартных проектов малого бизнеса. В его рамках можно использовать особые стандарты и спецификации, которые имеют минимальный перечень наиболее вероятных угроз, таких как вирусы, несанкционированный доступ, и другие.

Для выполнения более специфических требований к безопасности необходимо разрабатывать индивидуальный, повышенный режим безопасности [2]. Этот режим предусматривает стратегии работы с рисками разных классов, в которых реализуются следующие подходы:

– снижение рисков: многие риски могут быть снижены за счет использования простых и дешевых контрмер;
– неприятие риска: некоторые классы риска можно избежать с помощью выведения веб-сервера организации за пределы локальной сети;
– изменение характера риска: если невозможно уклониться от риска или уменьшить его, то лучше застраховать уязвимый объект;
– принятие риска: специалист должен знать остаточную ценность риска из-за невозможности сведения его к малой величине.

В результате, принимая во внимание все вышеперечисленные моменты, возможно создать достаточно эффективную систему риск-менеджмента для предприятия.

IV. Методы оценивания рисков в условиях политики информационной безопасности

Существует большое количество программ, для оценки рисков безопасности. Например, RA2 art of Risk, vsRisk, RiskWatch, COBRA, РискМенеджер, и многие другие.

С точки зрения использования таких программ в сфере малого бизнеса наилучших результатов с меньшими материальными затратами можно достичь с помощью методик OCTAVE-S и CRAMM.

Методы OCTAVE основаны на практических критериях OCTAVE, которые являются стандартными подходами для оценки ИБ. Данная методика реализуется вручную, без использования программных средств. Аналитическая команда, состоящая из 3-5 человек, рассматривает риски организационных активов в их соотношении с целями бизнеса. Конечным результатом метода является организацонно-направленная стратегия безопасности и план по смягчению последствий нарушений ИБ [3, 4].

В отличие от OCTAVE, CRAMM-CCTA Risk Analysis & Management реализуется с помощью специализированного программного обеспечения, которое можно настроить для различных отраслей. Текущая версия CRAMM 5 соответствует BS 7799 (ISO 17799).

Анализ рисков по методу CRAMM состоит из идентификации и расчета рисков на основе оценок определенных ресурсов, уязвимостей, угроз и ресурсов. Управление рисками с помощью CRAMM помогает выявить и выбрать контрмеры для снижения рисков предприятий рассматриваемых структур до приемлемого уровня [5].

Вывод

Согласно проведенному исследованию, информационная безопасность является чрезвычайно важным фактором корректного функционирования малого предприятия. Для его поддержания функционирования компании необходимо систематически проводить оценку рисков, анализ рисковых ситуаций, либо полный аудит предприятия.

Применение различных методов оценивания рисков в рамках риск-менеджмента позволяет обезопасить собственников предприятия от заранее предусмотренных рисков, а также способствует выработке методики защиты, отражения и принятия неучтенных рисков. Рассматриваемые подходы и приемы можно распространить на все типы предприятий малого бизнеса.

Список использованных источников

1. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность [Текст] / Петренко С.А., Симонов С.В. – М.: Компания АйТи; ДМК Пресс, 2004. – 384 с.: ил.
2. JetInfo, информационный бюллетень, вып. 1(68)/1999; [Текст]/М.:Джет Инфо Паблишер
3. Managing Risk: It's Not Just for Big Business, Stephen Townsend, IS 8930 Information Security Administration, Summer 2010,7/14/2010 [Electronic resource]: http://stephendtownsend.com/wordpress/wp-content/uploads/2010/12/
4. Stephen_Townsend_ResearchPaper2.pdf
5. Software Engineering Institute Carnegie Mellon [Electronic resource]: http://www.cert.org/octave/octaves.html
6. IT Expert [Electronic resource]: http://www.itexpert.ru/rus/ITEMS/77-33/index.php