Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.054

Фурса
Денис Артурович

Аудит сети предприятия

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1-45 80 02 «Телекоммуникационные системы и компьютерные сети»

_____

Научный руководитель
Лыньков Леонид Михайлович
доктор технических наук,
профессор

_____

Минск 2018

КРАТКОЕ ВВЕДЕНИЕ

Компания Itransition (ЗАО «Итранзишэн») является одним из ведущих разработчиков программного обеспечения в Республике Беларусь. Успехи на внешних рынках и открытие зарубежных офисов обусловили быстрый рост и успешное развитие компании. За период с 2006 по 2014 годы численность «Итранзишэн» увеличилась с 500 до 1400 сотрудников.

Компания Itransition работает с клиентами более чем из 30 стран мира. Накопленные за эти годы знания и опыт позволяют Itransition успешно работать в сфере разработки ПО и предлагать своим заказчикам качественные услуги и эффективные решения, а своим сотрудникам – перспективы развития и уверенность в завтрашнем дне.

Грамотная и всесторонняя зашита прав интеллектуальной собственности является необходимой для выживания компании и усиления ее позиций на рынке. Высокая динамика развития сетей связи и их интеграция с глобальными сетями, в том числе Интернетом, низкая стоимость средств вычислительной техники, уменьшение их габаритных размеров приводит к увеличению возможностей нарушителей для деструктивного воздействия на информационные ресурсы компании и нанесению материального ущерба. Положение усугубляется тем, что количество сотрудников компании и ее филиалов насчитывает более тысячи человек, каждый из которых может быть потенциальным нарушителем политики безопасности предприятия.

В этих условиях построенная в компании система управления информационной безопасностью должна периодически подвергаться независимому аудиту, который в соответствии с требованиями между народных стандартов является одним из обязательных этапов жизненного цикла данной системы.

Основным проблемным вопросом проведения аудита информационной безопасности является выбор сторонних организации для данной цели. Несмотря на то, что внешний аудитор может иметь лицензии, всегда остается вероятность использования сторонними специалистами обнаруженных уязвимостей для достижения своих корыстных целей. Разрешение данного противоречия является актуальной научной и практической задачей.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с научными исследования университета

Тема магистерской работы утверждена приказом ректора учреждения

образования «Белорусский государственный университет информатики и радиоэлектроники» протокол № 1 от 04.09.2017.

Цель и задачи исследования

Цель магистерской работы состоит в совершенствовании рекомендаций по проведению аудита информационной безопасности промышленного предприятия для снижения угроз утечки информации через сторонние организации.

Для достижения цели необходимо было решить следующие задачи:

1. Провести анализ структуры системы обеспечения информационной безопасности предприятия ЗАО «Итранзишэн»;
2. Исследовать подходы к аудиту информационной безопасности предприятия:
3. Разработать методику проведения внутреннего аудита информационной безопасности предприятия;
4. Разработать рекомендации по применению разработанной методики и апробировать их на предприятии ЗАО «Итранзишэн».

Объектом исследования явилась система обеспечения информационной безопасности предприятия ЗАО «Итранзишэн»

Предметом исследования выбран аудит информационной безопасности, позволяющий оценить уровень защищенности информационной системы предприятия ЗАО «Итранзишэн»

В качестве основных методов для решения поставленных задач применялись методы системного анализа, методы экспертного оценивания, теории вероятности и математической статистики.

Новизна полученных результатов

1. Развита теория аудита информационной безопасности иностранных предприятий в направлении разрешения противоречий между необходимостью предоставлять независимым аудиторам полную информацию об информационной системе предприятия, а также используемых механизмах обеспечения ее безопасности для повышения эффективности аудита и целесообразностью ограничить объем предоставляемых сведений из-за потенциальной вероятности использования аудиторами полученной информации в своих корыстных целях.
2. Усовершенствована методика проведения внутреннего аудита информационной безопасности предприятия.

Практическая значимость полученных результатов

1. Применение рекомендаций по применению методики внутреннего аудита информационной безопасности, разработанных в ходе работы, позволили определить направления улучшения системы обеспечения информационной безопасности предприятия. Помимо этого, реализация разработанных рекомендаций приведет к сокращению времени на проведение внутреннею периодическою аудита информационной безопасности до 21%, и увеличению на 19% скорости принятия решений при возникновении критических ситуаций, связанных с информационной безопасностью.

Основные положения выносимые на защиту

1. Методика проведения внутреннего аудита информационной безопасности предприятия основана на экспертном оценивании и обеспечивает расширение границ контроля информационной системы предприятия до 15%.
2. Модель системы обеспечения информационной безопасности предприятия ЗАО «Итранзишэн», позволяет сократить временные затраты на проведение периодического внутреннего аудита информационной безопасности до 21%, и увеличению на 19% скорости принятия решений при возникновении критических ситуаций, связанных с информационной безопасностью.

Апробация результатов диссертации

Основные положения диссертации обсуждались на 54-ой научной конференции аспирантов, магистрантов и студентов (Минск, 2018).

Опубликование результатов

Материалы результатов исследований, представленных в диссертации, опубликованы в 1 тезисе по материалам доклада на конференции [1-А].

Структура и объем работы

Диссертационная работа состоит из введения, общей характеристики работы, двух глав, заключения, библиографического списка и четырех приложений.

Общий объем диссертации составляет 86 страницы, включая 7 иллюстраций, 8 таблиц, список использованной литературы из 32 наименований и 4 приложений.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В главе 1 осуществлено обоснование места и роли аудита информационной безопасности предприятия. Важно отметить, что качества функционирования информационной сети зависит не только прибыль предприятия, но и его репутация.

Для противодействия возможным атакам злоумышленников построена система обеспечения информационной безопасности (СОИБ).

Непрерывное развитие сетевых технологий при отсутствии постоянно проводимого анализа их безопасности приводит к тому, что с течением времени защищенность предприятия от внутренних и внешних угроз падает, т.к. появляются новые неучтенные угрозы и уязвимости, противопоставить которым нечего.

Следует отметить, что оценка уровня информационной безопасности ИС предприятия, сопоставление его с объективно необходимым уровнем, а в случае несоответствия подбор оптимального комплекса зашиты представляет собой весьма непростую и дорогостоящую задачу.

Созданная на предприятии ЗАО «Итранзишэн» система обеспечения информационной безопасности в настоящее время не в полной мере соответствует современным требованиям и нуждается в совершенствовании. Отсутствие подразделений, отвечающих за аудит информационной безопасности не позволяет объективно оценивать защищенность информационных ресурсов и информационной инфраструктуры от внутренних и внешних угроз и принимать адекватные меры по их нейтрализации. Кроме того, из-за потенциальной опасности использования внешними аудиторами выявленных уязвимостей СОИБ в своих корыстных целях, сторонние организации не могут быть привлечены для оценки текущего состояния защищенности предприятия.

Также в первой главе представлены этапы проведения аудита с их кратким описанием. Помимо этого для каждого этапа приведен список задач, которые необходимо решить в ходе его проведения.

Представлен перечень исходных данных, необходимых для аудита ИБ, список вопросов, ответы на которые должен получить аудитор в ходе анализа этих данных. Приведены 2 подхода для анализа данных и их описание – использование стандартов информационной безопасности и использование методов анализа рисков.

Произведён аналитический обзор литературы в области информационной безопасности в результате которого были выявлены подходы к классификации

аудита информационной безопасности. Представлена их обобщенная классификация с описанием каждого подхода.

Представлены различные программные продукты для анализа рисков, которые могут использоваться в ходе аудиторской проверки информационной безопасности предприятия: CRAMM, RiskWatch, COBRA, Buddy System. Сделано их краткое описание и сравнение.

Глава номер 2 посвящена разработке методики проведения независимого внутреннего аудита информационной безопасности предприятия.

Из-за большого количества и разнообразного характера неопределенностей, чрезвычайной сложности и значительных масштабов, сопровождающих аудит информационной безопасности предприятия, предпочтение было отдано методу экспертных оценок.

Описан процесс проведения экспертного опроса: какие этапы он включал, процесс и принцип формирования группы экспертов, оценка информированности эксперта о рассматриваемой проблеме. Приведен фрагмент анкеты оценки информированности экспертов.

Сформированной группе экспертов были предложены анкеты с целью ответов на вопросы о соответствии созданной системы обеспечения информационной безопасности предприятия современным требованиям.

Анкетирование проводилось анонимно, что позволило избежать давления на мнение экспертов и получить независимые субъективные мнения экспертов по рассматриваемой задаче.

Описаны выводы, которые были получены в результате обработки результатов опроса экспертов.

С целью устранения недостатков присущих СОИБ, выявленных в предыдущих разделах, была разработана методика проведения независимого внутреннего контроля.

Проведенный экспертный опрос опенки, достоинств разработанной методики проведения внутреннего аудита информационной безопасности предприятия, показал, что ее применение позволяет расширить границы контроля информационной системы предприятия до 15%.

Даны рекомендации по совершенствованию системы обеспечения информационной безопасности предприятия. Для уменьшения стоимости системы информационной безопасности, желательно в первую очередь выполнять только те мероприятия, которые направлены на минимизацию наиболее вероятных и опасных рисков. Данный подход позволяет направить

финансовые ресурсы именно на повышение уровня информационной безопасности, и четко отслеживать эффективность вложений.

Отметим, что система обеспечения информационной безопасности должна быть встроена в деятельность компании, иначе ее эффективность будет минимальной. Построение данной системы требует перестроения безнес-процессов компании и добавление функции обеспечения и контроля информационной защиты.

Для повышения качества обеспечения информационной безопасности предприятия ЗАО «Итранзишэн» предлагается в состав СОИБ включить службу внутреннего аудита.

Проведенные исследования показали, что наибольшая эффективность СОИБ по противодействию внутренним и внешним угрозам может быть достигнута при реализации процессного подхода к аудиту информационной безопасности, в основе которой лежит процессная модель Деминга.

Для эффективного обеспечения информационной безопасности предприятия целесообразно уделять внимание повышению квалификации как пользователей, так и сотрудников службы аудита, службы автоматизации и программирования и службы безопасности. При этом важно, чтобы обучение проводилось с максимальной отдачей и минимальными вложениями.

Следует отметить, что в течение первого полугодия с момента внедрения предложенной СОИБ необходимо ежемесячно тестировать процедуры аудита. Это позволит исключить ошибки, допущенные при разработке. В дальнейшем тестирование системы внутреннего аудита может проводиться раз в пол года.

ЗАКЛЮЧЕНИЕ

Проведения аудита безопасности предприятия дает возможность обеспечить формирование единой политики и концепции безопасности предприятия; рассчитать, согласовать и обосновать необходимые затраты на защиту предприятия; объективно и независимо оценить текущий уровень информационной безопасности предприятия; обеспечить требуемый уровень безопасности и в целом повысить экономическую эффективность предприятия; эффективно создавать и использовать профили защиты конкретного предприятия на основе неоднократно апробированных и адаптированных качественных и количественных методик оценки информационной безопасности предприятий заказчика.

Созданная система обеспечения информационной безопасности предприятия ЗАО «Итранзишэн» позволяет своевременно выявлять каналы

утечки конфиденциальной информации и принимать меры по их нейтрализации. Вместе с тем развитие информационных и телекоммуникационных технологий при отсутствии постоянно проводимого анализа их безопасности вследствие высокой загрузки специалистов службы безопасности и службы автоматизации и программирования приводит к тому, что система обеспечения информационной безопасности в настоящее время не в полной мере соответствует современным требованиям и нуждается в совершенствовании.

Разработана методика проведения внутреннего аудита информационной безопасности предприятия, основанная на экспертном оценивании и обеспечивающая расширение границ контроля информационной системы предприятия до 15%. С использованием положений методики разработаны рекомендации позволяющие сформировать облик перспективной системы обеспечения информационной безопасности предприятия ЗАО «Итранзишэн», практическая реализация которого приведет к сокращению временных затрат на проведение внутреннего периодического аудита информационной безопасности до 21%, а также повышению оперативности принятия решений при возникновении кризисных ситуаций в области информационной безопасности на 19%.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А Фурса, Д.А. Аудит IT-инфраструктуры / Д.А. Фурса // Телекоммуникационные системы и сети: материалы 54-й научной конференции аспирантов, магистрантов и студентов (Минск, 23 –27 апреля 2018 г.). – Минск: БГУИР, 2018.