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

УДК 681.3.06

Ковалев
Владислав Владимирович

Программное средство для аудита систем защиты информации предприятия

АВТОРЕФЕРАТ ДИССЕРТАЦИ
на соискание степени магистра технических наук
по специальности 1-98 80 01 Методы и системы защиты информации, информационная безопасность

_____

Научный руководитель
Боднарь Иван Васильевич
докт. хим. наук, профессор

_____

Минск 2017

Библиотека БГУИР

ВВЕДЕНИЕ

В настоящее время управление информационными рисками представляет собой одно из наиболее актуальных и динамично развивающихся направлений стратегического и оперативного менеджмента в области защиты информации. Его основная задача – объективно идентифицировать и оценить наиболее значимые для бизнеса информационные риски компании, а также адекватность используемых средств контроля рисков для увеличения эффективности и рентабельности экономической деятельности компании. Поэтому под термином «управление информационными рисками» обычно понимается системный процесс идентификации, контроля и уменьшения информационных рисков компаний в соответствии с определенными ограничениями российской нормативно правовой базы в области защиты информации и собственной корпоративной политики безопасности. Считается, что качественное управление рисками позволяет использовать оптимальные по эффективности и затратам средства контроля рисков и средства защиты информации, адекватные текущим целям и задачам бизнеса компании.

Сегодня наблюдается повсеместное усиление зависимости успешной бизнес деятельности отечественных компаний от используемых организационных мер и технических средств контроля и уменьшения риска. Для эффективного управления информационными рисками разработаны специальные методики, например методики международных стандартов ISO 15408, ISO 17799 (BS7799), BSI; а также национальных стандартов NIST 800-30, SAC, COSO, SAS 55/78 и некоторые другие, аналогичные им. В соответствие с этими методиками управление информационными рисками любой компании предполагает следующее. Во-первых, определение основных целей и задач защиты информационных активов компании. Во-вторых, создание эффективной системы оценки и управления информационными рисками. В-третьих, расчет совокупности детализированных не только качественных, но и количественных оценок рисков, адекватных заявленным целям бизнеса. В-четвёртых, применение специального инструментария оценивания и управления рисками. Рассмотрим некоторые качественные и количественные международные методики управления информационными рисками, обращая основное внимание на возможность их адаптации и применения в отечественных условиях.

Библиотека БГУИР

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Цель диссертационной работы – исследование методик проведения аудиторской компании в организациях и разработка программного обеспечения для проведения аудита по защите информации в организации.

Для достижения поставленной цели были решены следующие задачи.

1. Проведен анализ современных стандартов, нормативных и правовых актов, регламентирующие аудит систем защиты информации предприятий.
2. Выполнен сравнительный анализ существующих методик и программных средств, используемых аудита систем защиты информации.
3. На основе результатов проведенного сравнительного анализа стандартов, нормативных актов и существующих методик разработано программное обеспечение для проведения аудита систем защиты информации предприятий.

Предмет исследования – СТБ ISO/IEC 27001-2011, СТБ ISO/IEC 27002-2012, СТБ ISO/IEC 27005-2011, СТБ ISO/IEC 17799-2005, Приказ ОАЦ при Президенте Республики Беларусь от 16.01.2015 № 3.

Личный вклад соискателя

Все основные результаты, изложенные в диссертационной работе, получены автором самостоятельно. Научный руководитель, доктор химических наук, профессор И.В. Бондарь принимал участие в планировании работы и обсуждении ее результатов.

Апробация результатов диссертации

Результаты диссертационной работы докладывались и обсуждались на XII Международной научно-практической конференции «Управление информационными ресурсами» (Минск, 9 декабря 2016 г.), 53-й конференции аспирантов, магистрантов и студентов БГУИР (Минск, 2–6 мая 2017 г.), XV Белорусско-российской научно-технической конференции «Технические средства защиты информации» (Минск, 6 июня 2017 г.).

Библиотека БГУИР

ЗАКЛЮЧЕНИЕ

Проанализированы и сравнены различные методики аудита систем защиты информации (COBRA, КОНДОР+, RA Software Tool, CRAMM, MethodWare). Для каждой из данных методик уже существует разработанные программные средства для проведения аудиторской компании в различных компаниях с возможностью гибкой настройки. Определено, что главной недостаток этих методик – большой объем используемых документов.

На основе проведенного сравнения были установлены основные, общие функциональности и подходы проведения аудита системы защиты информации. Разработан упрощенный алгоритм проведения аудита системы защиты информации организации, с применением которого могут быть выявлены основные причины уязвимостей этой системы. Упрощение алгоритма обусловлено применением в ходе аудита разработанного программного средства. Основные его преимущества по сравнению с аналогами – простота запуска и настройки; независимость от типа операционной системы; возможность получения доступа как через локальную сетб, а так с использованием туннельного подключения VPN. Указанные преимущества избавляют аудитора или сотрудника аудируемой организации от необходимости выполнения ручной установки, а руководителя этой организации – от необходимости выделения отдельного помещения для проведения аудита, а также от закупки дополнительного оборудования для этих целей.

Библиотека БГУИР

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1. Ковалёв, В.В. Актуализация разработки программного средства для проведения аудита системы защиты информации организаций электросвязи / В.А. Бойправ, Л.Л. Утин, В.В. Ковалев // Управление информационными ресурсами : тез. докл. XIII Междунар. научн.-практ. конф. Минск, 9 декабря 2016 г. – С. 181–182.

2. Ковалёв, В.В. Особенности анкетирования сотрудников организаций электросвязи при проведении аудита системы менеджмента защиты информации / В.А. Бойправ, Л.Л. Утин, В.В. Ковалёв // Технические средства защиты информации : тез. докл. XV Белорусско-российской научно-технической конференции. Минск, 6 июня 2017 г. – Минск: БГУИР, 2017. – С. 13–14.

Библиотека БГУИР