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

УДК_____

Пимошенко
Михаил Юрьевич

Аудит информационной безопасности ОАО «Белсвязьстрой»

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1-45 81 01 «Инфокоммуникационные системы и сети»

_____

Научный руководитель
Пулко Татьяна Александровна

к.т.н., доцент

_____

Минск 2017

КРАТКОЕ ВВЕДЕНИЕ

Актуальность проблемы защиты информации сегодня не вызывает сомнений. Успех современной компании и ее развитие в условиях острой конкуренции в значительной степени зависят от применения информационных технологий, а следовательно, от степени обеспечения информационной безопасности.

Любое предприятие располагает различными видами информации, представляющими интерес для злоумышленников. Прежде всего, это коммерческие данные, информация, являющаяся интеллектуальной собственностью предприятия и конфиденциальные данные.

Поэтому защите информации от неправомерного овладения ею отводится весьма значительное место. При этом "целями защиты информации являются: предотвращение разглашения, утечки и несанкционированного доступа к охраняемым сведениям; предотвращение противоправных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы; обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах; сохранение государственной тайны, конфиденциальности документированной информации в соответствие с законодательством; обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологии и средств их обеспечения".

Политика информационной безопасности - свод документов, в которых рассматриваются вопросы организации, стратегии, методов и процедур в отношении конфиденциальности, целостности и доступности информационных ресурсов предприятия. Политика безопасности строится на основе анализа рисков - процесса определения угроз безопасности системы и отдельным ее компонентам, определение их характеристик и потенциального ущерба.

Конечная цель разработки политики информационной безопасности - обеспечить целостность, доступность и конфиденциальность для каждого информационного ресурса.

Исследуемое предприятие ОАО «Белсвязьстрой» циркулирует большое количество информации конфиденциального характера, доступ к которой необходимо ограничить. Поэтому целью будет являться разработка такой системы по защите информации, при которой угрозы утечки конфиденциальной информации будут минимальны.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цели и задачи исследования

Цель диссертационной работы заключалась в исследовании возможности применения существующих методов проведения аудита информационной безопасности на предприятии связи ОАО «Белсвязьстрой», разработке и внедрении способов повышения безопасности при работе в сети и своевременного обнаружения входящих и исходящих угроз безопасности. Для достижения поставленной цели потребовалось решение следующих задач:

1. Провести анализ существующей политики безопасности на предприятии.
2. Выявить недостатки в существующей политике безопасности.
3. Разработать и внедрить методы повышения безопасности при работе в сети и своевременного обнаружения входящих и исходящих угроз.

В качестве объекта исследования рассматривалось предприятие связи ОАО «Белсвязьстрой»

Предметом исследований являлись информационные ресурсы предприятия.

Апробация и опубликованность результатов

Основные полученные результаты диссертационной работы докладывались и обсуждались на 52 научной конференции аспирантов, магистрантов и студентов Белорусского государственного университета информатики и радиоэлектроники; XIV Белорусско-российской научно-технической конференции «Технические средства защиты информации».

Структура и объем диссертации

Диссертационная работа состоит из краткого содержания работы, введения, четырех глав, заключения и библиографического списка. Полный объем диссертации составляет 71 страницу машинописного текста. Диссертация содержит 2 рисунка, 6 таблиц, 1 приложение. Библиографический список занимает 3 страницы и состоит из 37 наименования использованных источников и списка собственных публикаций соискателя из двух наименований на одной странице.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении описываются цели аудита информационной безопасности, актуальность работы, формулируются решаемые в магистерской диссертации задачи.

В первой главе работы рассмотрены основные теоретические аспекты. Рассмотрены методы оценки защищенности информационных систем. Приведены примеры защиты информации. Рассмотрены методы обеспечения информационной безопасности.

Во второй главе проведен анализ нормативно-правовой базы в области политики безопасности Республики Беларусь. Рассмотрены законы, указы, постановления в области информационной безопасности Республики Беларусь. Проведен анализ стандартов информационной безопасности. Сделаны выводы о полезности аудитов информационной безопасности на предприятии.

В третьей главе рассмотрены основные этапы проведения аудита информационной безопасности на предприятии. Приведена разработка регламента внутреннего аудита. Рассматриваются методы, которые применяются для сбора исходных данных аудита информационной безопасности. Дана оценка уровня безопасности информационных систем. Сделаны выводы по результатам аудита безопасности.

В четвертой главе рассмотрена структура организации, проанализированы основные проблемы, связанные с информационной безопасностью. Как результат сформированы рекомендации по обеспечению должного уровня информационной безопасности. Так же рассмотрены меры для предотвращения дальнейших инцидентов, связанных с нарушением информационной безопасности.

В заключении приводятся основные результаты, полученные в ходе выполненных исследований.

ЗАКЛЮЧЕНИЕ

Проведенное исследование позволило сделать следующие выводы и сформулировать рекомендации для безопасной работы в сетях.

Установлено, что основной причиной проблем предприятия в области защиты информации является отсутствие политики обеспечения информационной безопасности, которая включала бы организационные, технические, финансовые решения с последующим контролем их реализации и оценкой эффективности.

Проведенный анализ системы информационной безопасности выявил существенные недостатки, в числе которых:

- хранение резервных копий в серверной, резервный сервер находится в одном помещении с основными серверами;
- отсутствие надлежащих правил в отношении парольной защиты (длина пароля, правила его выбора и хранения);
- администрированием сети занимается один человек.

Обобщение международной и национальной практики в области управления информационной безопасностью предприятий позволило заключить, что для ее обеспечения необходимы:

- категорирование информации (на служебную или коммерческую тайну);
- прогнозирование и своевременное выявление угроз безопасности, причин и условий, способствующих нанесению финансового, материального и морального ущерба;
- создание условий деятельности с наименьшим риском реализации угроз безопасности информационным ресурсам и нанесения различных видов ущерба;

Обеспечение информационной безопасности организации – это непрерывный процесс, требующий постоянного контроля. И естественно сформированная политика не является железным гарантом защиты. Помимо внедрения политики нужен постоянный контроль за ее качественным исполнением, а так же совершенствованием в случае каких-либо изменений в компании или прецедентов. Для организации рекомендовано было взять в штат так же сотрудника, деятельность которого будет напрямую связана с этими функциями (администратор защиты) Так же на предприятии внедрена программы системы мониторинга DUDE.

Построение грамотной методики обеспечения информационной безопасности в каждом конкретном случае, с учетом всех внутренних и внешних факторов позволит создать действительно эффективную систему информационной безопасности, обеспечивая достаточный уровень защиты.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. Пимошенко М.Ю. Оценка текущего состояния системы информационной безопасности предприятия / М.Ю. Пимошенко, Т.А. Пулко // XIV Белорусско-российская научно-техническая конференция «Технические средства защиты информации»: Тезисы докладов – Минск, 2016 – с.67

2-А. Пимошенко М.Ю. Аудит информационной безопасности ОАО «Белсвязьстрой» / М.Ю. Пимошенко, Т.А. Пулко // 52-ая научная конференция аспирантов, магистрантов и студентов Белорусского государственного университета информатики и радиоэлектроники.