Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет

Информатики и радиоэлектроники

УДК_____

Атбаканов

Максим Сергеевич

Аудит информационной безопасности сети передачи данных на примере ГУ «Главное хозяйственное управление»

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

Научный руководитель

Гасенкова Ирина Владимировна
доктор физико-математических наук, профессор

Минск 2017

ВВЕДЕНИЕ

Аудит информационной безопасности представляет собой независимую и объективную оценку текущего состояния защищенности информационной системы, позволяющую систематизировать угрозы информационной безопасности и предложить рекомендации по их устранению.

Результаты аудита позволяют установить соответствие уровня защищенности информационной системы выдвигаемым требованиям, необходимым параметрам конфиденциальности, целостности и доступности ресурсов информационной системы.

Аудит собственных систем защиты информации организации позволяет дать независимую и объективную оценку защищенности информационной системы от внутреннего несанкционированного воздействия и утечки конфиденциальной информации.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Диссертационная работа посвящена разработке методики и проведению аудита информационной безопасности сети передачи данных (СПД). Аудит - процесс сбора и анализа информации об информационной системе для качественной или количественной оценки уровня ее защищенности от атак злоумышленников.

В настоящее время аудит информационной безопасности представляет собой одно из наиболее актуальных и динамично развивающихся направлений стратегического и оперативного управления в области безопасности корпоративных систем. Его основная задача - объективно оценить текущее состояние информационной безопасности компании, а также ее адекватность поставленным целям и задачам бизнеса с целью увеличения эффективности и рентабельности экономической деятельности компании. Считается, что результаты качественно выполненного аудита информационной безопасности компании позволяют построить оптимальную по эффективности и затратам корпоративную систему защиты, адекватную ее текущим задачам и целям.

Спектр угроз для ИС расширился. Это обусловлено передачей информации по сетям общего пользования, «информационными войнами», высокой «текучкой» кадров. Проведение аудита позволяет оценить текущее состояние безопасности функционирования сети, «выделить» риски, прогнозировать и управлять ими, корректно подойти к вопросу обеспечения безопасности информационных активов организации.

В результате организации предлагается комплексный план внесения изменений в систему управления информационной безопасностью как для повышения реального уровня защищенности, так и для соответствия принятым стандартам.

В данной работе был проведен аудит информационной безопасности сети передачи данных Государственного учреждения «Главное Хозяйственное Управление» Управления делами Президента Республики Беларусь. Данное учреждение предоставляет услуги в том числе и органам государственного управления, что вынуждает уделять серьезное внимание вопросам информационной безопасности.

Анализ СПД ГХУ производился на основании предоставленных схем СПД, конфигураций активного оборудования сети, данных с систем мониторинга и иной информации, предоставленной инженерами отдела вычислительных систем и администрирования центра информационных технологий ГХУ и рекомендаций и постановлениями Операционно-аналитического центра при Президенте Республики Беларусь.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Государственное учреждение "Главное хозяйственное управление" Управления делами Президента Республики Беларусь (ГХУ) было создано в целях надлежащего управления государственной собственностью. Обеспечивает эффективное использование около 400 зданий и сооружений, размещает республиканские органы управления. Сдает в аренду помещения в административных зданиях столицы и областных центров. Обеспечивает работу органов государственного управления. Поэтому вопросы защиты передаваемой информации имеют большое значение.

Целью аудита сети передачи данных (СПД) Государственного учреждения «Главное Хозяйственное Управление» Управления делами Президента Республики Беларусь является:

1. Проверка версий программного обеспечения (ПО) активного оборудования СПД на наличие устаревших версий, а также на наличие версий ПО активного оборудования, имеющих существенные уязвимости;
2. Проверка «жизненного цикла» активного оборудования СПД. В результате данной проверки мы определим наличие в СПД оборудования, которое более не производится и не поддерживается производителем, либо установлена дата окончания производства и поддержки данного активного оборудования;
3. Анализ архитектуры СПД, позволяющий определить слабые стороны эксплуатируемой СПД, потенциальные проблемы, обусловленные данной архитектурой и, как результат, рекомендации по реорганизации архитектуры СПД для устранения выявленных недостатков и обеспечения возможности дальнейшего развития сетевой инфраструктуры.

Анализ СПД ГХУ производился на основании предоставленных схем СПД, конфигураций активного оборудования сети, данных с систем мониторинга и иной информации, предоставленной инженерами отдела вычислительных систем и администрирования центра информационных технологий ГХУ.

ГУ «ГХУ» является государственной организацией предоставляющей услуги органам государственного управления. В связи с этим, при проведении аудита, мы руководствовались рекомендациями и постановлениями Операционно-аналитического центра при Президенте Республики Беларусь (далее ОАЦ).

ОАЦ является государственным органом, осуществляющим регулирование деятельности по обеспечению защиты информации, содержащей сведения, составляющие государственные секреты Республики Беларусь или иные сведения, охраняемые в соответствии с

законодательством, от утечки по техническим каналам, несанкционированных и непреднамеренных воздействий.

Рекомендации ОАЦ по обеспечению безопасности информации в локальных сетях, подключенных к сети Интернет

Государственные органы обязаны реализовать в собственных информационных системах и контролировать выполнение подчиненными организациями меры, позволяющие:

- осуществлять предоставление доступа сотрудникам органа (организации) к сервисам сети Интернет (электронная почта, передача файлов, информационные ресурсы и др.) в соответствии с определенным в государственном органе порядком;
- определить правила работы сотрудников с сервисами сети Интернет (электронная почта, передача файлов, доступ к информационным ресурсам, IP-телефонии, социальным сетям и публичным системам мгновенных сообщений);
- определить администраторов сети, их права и обязанности;
- определить права и обязанности пользователей;
- определить ответственность сотрудников и должностных лиц за обеспечение защиты информации;
- обеспечить контроль использования сотрудниками в глобальных сетях: IP-телефонии, социальных сетей и публичных систем мгновенных сообщений;
- определить порядок и перечень используемого программного обеспечения на средствах вычислительной техники сотрудников;
- определить порядок применения средств защиты информации, установленных в локальной вычислительной сети;
- определить необходимые мероприятия по разграничению доступа к средствам защиты информации и обработки информации;
- определить регламент смены атрибутов безопасности (паролей) пользователей;
- определить порядок действий при возникновении нештатной ситуации (сбои, повреждения и отказы) с информационными ресурсами;
- определить регламенты резервирования и уничтожения информации;
- определить порядок контроля, учета использования ресурсов сети Интернет пользователями, формирования и предоставления руководству организации отчетных документов.

С использованием технических, программно-аппаратных и программных средств:

- обеспечить межсетевое экранирование с использованием собственных возможностей и (или) возможностей уполномоченных поставщиков интернет-услуг;
- обеспечить идентификацию абонентских устройств в локальной сети;
- обеспечить блокирование неконтролируемого обмена информацией между рабочими местами пользователей в локальной сети;
- исключить использование на рабочих местах в локальной сети постороннего программного обеспечения, ресурсов сети Интернет, предназначенных для сокрытия действий пользователя;
- исключить подключение рабочего места в локальной сети к сетям связи общего пользования через другие каналы доступа (сотовый телефон, модем);
- обеспечить синхронизацию системного времени от единого (общего) источника (в качестве источника использовать службу единого времени Белорусского государственного института метрологии);
- осуществлять сбор и хранение данных авторизации и статистики использования сети Интернет пользователями в течение 1 года;
- обеспечить возможность анализа использования сети Интернет пользователями (с использованием собственных возможностей или поставщиков интернет-услуг);

применять криптографические протоколы для защиты данных авторизации при работе с сервисами сети Интернет.

Основные выводы по результатам аудита

СПД ГУ «Главное Хозяйственное Управление» на момент проведения аудита по многим критериям не соответствует рекомендованной компанией Cisco архитектуре корпоративных сетей передачи данных:

– использование в сети оборудования большого числа различных производителей;

– наличие в сети большого числа оборудования, снятого с поддержки производителем;

– минимальная отказоустойчивость сегментов СПД, вызванный как физической топологией отдельных сегментов, так и применяемыми настройками, а также используемыми технологиями;

– отсутствует единый структурный (уровневый) подход в дизайне СПД, роль многих сетевых устройств не имеет четкого определения и назначения;

– отсутствие типовых технических решений затрудняет масштабируемость сетевой инфраструктуры и усложняют ее эксплуатацию;

– недостаточный уровень безопасности в сети и в конфигурациях сетевых элементов может привести к опасным инцидентам;

– отсутствует единое централизованное управление сетью;

– настройки разных сегментов сети не имеют единых правил и политик;

– отсутствуют типовые шаблоны конфигурации устройств.

ЗАКЛЮЧЕНИЕ

Наиболее взвешенным решением для текущей архитектуры сети, является разработка новой архитектуру СПД на основании модульного принципа построения сетей передачи данных, обеспечивающего максимальную гибкость, масштабируемость сети, а также упрощает её текущую эксплуатацию.

За основу следует взять уже сформированные логические модули СПД ГХУ, описанные в общих сведениях:

- Интернет модуль;
- Модуль подключения ведомственных сетей;
- Центр обработки данных (ЦОД);
- Сеть сотрудников ГХУ.

Каждый из приведённых выше модулей должен иметь чёткие границы. Внешний периметр каждого модуля должен бать защищён парой устройств безопасности (межсетевой экран «нового поколения» с расширенными функциями, список которых зависит от защищаемого им модуля сети), обеспечивающей защиту внутренней инфраструктуры модуля, а также контроль доступа. Все основные устройства каждого из модулей должны дублироваться только для обеспечения отказоустойчивости.

По максимуму исключить использование устройств, снятых с поддержки их производителем.

В сети передачи данных максимально должны использоваться протоколы динамической маршрутизации с включенной функцией суммированием адресов.

Внутри модулей необходимо осуществить подсетей на основании функциональных обязанностей пользователей, их территориального размещения, групп сервисов центра обработки данных, технических нужд.

Необходимо обеспечить контроль версий ПО, установленного на активном сетевом оборудовании.

Сеть должна иметь единую систему управления и мониторинга.

Должны быть разработаны документы и процессы, стандартизирующие как конфигурации оборудования, так и процесс текущей эксплуатации СПД ГУ ГХУ.