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

УДК 658.048

Кемежук

Марина Михайловна

Методы и средства обеспечения непрерывности функционирования ИТ-сервисов и систем в условиях чрезвычайной ситуации

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1-94-80-01 Предупреждение и ликвидация чрезвычайных ситуаций

_____

Научный руководитель
Мельниченко Дмитрий Александрович
кандидат технических наук, доцент

_____

Минск 2015

ВВЕДЕНИЕ

Сегодня общая стабильность работы многих компаний и производств в мире обусловлена непрерывностью и стабильностью работы их аппаратных и программных средств хранения, обработки информации. Базы данных, ИТ-сервисы – все это обеспечивает бесперебойную работу компании, как в обычном режиме, так и в случае возникновения чрезвычайной ситуации.

Необходимо отметить, что в зарубежных компаниях обеспечение непрерывности бизнеса не входит в сферу ответственности ИТ, в большинстве случаев это задача генеральных директоров и риск-менеджмента. Таким образом, приветствуется комплексный подход к обеспечению непрерывности работы бизнес-организаций, работа которых построена на использовании компьютерных и сетевых ресурсов. Необходимо отметить, что данный подход составления планов и стратегий обеспечения непрерывности работы ИТ-систем для нашей страны является достаточно новым.

Проведя анализ, можно с уверенностью сказать, что чрезвычайные ситуации в мире возникают все чаще. Это связано с интенсивным освоением мира человеком, широким использованием природных ресурсов, расширением техногенных процессов. Возникновение той или иной чрезвычайной ситуации может оказать значительное влияние на стабильность работы компании, в некоторых случае привести к потере информации и полной остановке работы организации.

Возникновение любой другой чрезвычайной ситуации, будь то отключение электроэнергии в результате грозы, угроза подтопления, обрыв линий электропередач в результате сильного ветра, хакерская атака – все это может привести к сбоям в работе ИТ-систем и сервисов, которые являются критичными для функционирования многих организаций, включая банки, государственный аппарат и финансовый сектор.

Очевидна зависимость бизнеса от эффективной работы ИТ-инфраструктуры, непрерывность работы бизнес-приложений, стала вопросом жизнеспособности компаний. В данных условиях вопрос обеспечения непрерывности работы ИТ-сервисов и систем в условиях чрезвычайной ситуации является более чем актуальным.

ОБЩАЯ ХАРАКТЕРИСТРИКА РАБОТЫ

В современном обществе роль информационных технологий постоянно возрастает. Сегодня большинство предприятий успешно организуют свою деятельность, благодаря использованию информационных технологий и ресурсов, поэтому безопасность, надежность и бесперебойность работы ИТ-сервисов и систем носит приоритетный характер. ИТ-сервисы должны продолжать свою работу во время чрезвычайных ситуации или быстро восстанавливать свою работоспособность при ликвидации последствий чрезвычайных ситуаций. Не является исключением и банковский сектор.

На сегодняшний день одним из приоритетных направлений обеспечения стабильности работы в банковском секторе и системе взаимодействия государственных учреждений является надежная передача конфиденциальной информации, защищенность персональных данных клиентов, возможность оказывать услуги в режиме 24x7. Поэтому актуальным остается вопрос организации защищенной передачи конфиденциальной информации в реальном масштабе времени с возможностью удобной обработки информации служащими банковской системы.

Основной целью магистерской диссертации является разработка схемы защищенной сети для межбанковского обмена информацией, анализ методов и средств обеспечения непрерывности работы ИТ-сервисов. Для достижения цели были поставлены следующие задачи:

1. Изучить основные методы и средства обеспечения непрерывности работы ИТ-сервисов;
2. Провести анализ используемых технологий защиты и восстановления данных;
3. Разработать организационные методы защиты данных;
4. Изучить теоретические основы технологий защиты информации;
5. Выбрать производителя, оборудование и программное обеспечение разрабатываемой сети;
6. Разработать проект защищенной сети межбанковского обмена конфиденциальной информацией.

Основными положениями, выносимыми на защиту магистерской диссертации, являются технологии защиты информации, применяемые в сетях передачи данных, организационные методы защиты данных в случае возникновения внештатной ситуации, программные и аппаратные средства резервирования элементов и информационных ресурсов сети. Результатом работы является проект защищенной сети обмена информацией в банковском

секторе, в основе которого лежат современные технологии защиты информации, средства по предупреждению несанкционированного доступа в сеть, а также возможность использования специализированного программного обеспечения, обладающего встроенными средствами шифрования и имеющего удобный интерфейс взаимодействия с системой.

Основные результаты работы были представлены и опубликованы в сборниках следующих конференций:

1. XVIII Международная научно-практическая конференция «Современные средства связи». Высший государственный колледж связи, 2013г.;

2. Международная научно-техническая конференция, приуроченная к 50-летию МРТИ-БГУИР. Белорусский государственный университет информатики и радиоэлектроники, 2014г.;

3. XIX Международная научно-практическая конференция «Современные средства связи». Высший государственный колледж связи, 2014г.

Диссертационная работа состоит из трех глав, первая из которых представляет собой обзор технологий защиты информации. Вторая глава включает в себя подробное изучение методов и средств обеспечения непрерывности функционирования ИТ-сервисов и систем в условиях чрезвычайной ситуации. Каждая из глав разбита на подразделы, что позволяет последовательно изложить материал диссертации.

Текст диссертационной работы занимает 80 страниц машинописного текста и включает в себя 36 рисунков, 3 таблицы. При подготовке работы были использованы 34 литературных источника.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Текст диссертационной работы включает в себя три главы. Первая глава представляет собой обзор технологий защиты информации. В данной главе приводится определение понятия чрезвычайной ситуации, а также базовая классификация чрезвычайных ситуаций. На основании данной классификации выделяются основные чрезвычайные ситуации, характерные для нашей страны. Исходя из этого, формируется перечень чрезвычайных ситуаций, которые могут повлиять на работу ИТ-сервисов и систем.

В данной главе, опираясь на данные литературных источников, в хронологическом порядке собрана информация о развитии средств и методов защиты информации, а также приводится структура системы защиты информации, применяемой в общемировой практике.

Вторая глава включает в себя методы и средства обеспечения непрерывности функционирования ИТ-систем и сервисов в условиях чрезвычайной ситуации. Особое внимание уделяется анализу наиболее известных западных стандартов управления непрерывностью бизнеса, основанного на использовании ИТ-сервисов. Внедрение данных стандартов на предприятиях является достаточно новым для нашей страны явлением, так как не все ИТ-структуры имеют подразделения специалистов, основной задачей которых является разработка планов непрерывности бизнеса.

В данной главе также проводится анализ существующих технологий защиты и восстановления данных. В ходе анализа выделяются преимущества и недостатки изучаемых технологий. Анализируются также методы защиты информации, приводятся их достоинства и недостатки, предлагается выбрать наиболее подходящий метод защиты информации в сети обмена конфиденциальной информацией. Последний подраздел главы включает в себя разработку организационных мер по защите ИТ-сервисов в условиях чрезвычайной ситуации.

В третьей главе производится разработка схемы межбанковского обмена конфиденциальной информацией. Осуществляется выбор производителя оборудования разрабатываемой сети. В нашем случае используется оборудование компании Cisco – флагмана среди производителей сетевого оборудования. Особое внимание уделяется выбору программного обеспечения. В разрабатываемой сети используется разработка белорусского предприятия ОАО «ЦБТ». Необходимо обметить, что на территории Республики Беларусь ни один из разработчиков программного обеспечения не предлагает возможных аналогов данной системе в том виде, в котором она существует. Нет аналогов и на территории РФ, поэтому «Система

гарантированной доставки сообщений» является своего рода уникальной разработкой.

В данной главе подробно рассмотрен процесс обработки и передачи сообщений в системе, приводятся рисунки пользовательского интерфейса, и административной части.

Особое внимание уделено настройке репликации транзакций – как средству резервирования и программного восстановления данных.

Результатом работы является разработка схемы межбанковского обмена конфиденциальной информацией, где ядро сети строится на основе оборудования Cisco, рабочие места пользователей сетей банков включаются в ядро сети посредством межсетевого экрана. Соединение сетей осуществляется с помощью высокоскоростных оптоволоконных магистральных линий. Приводится структурная схема организации связи, а также схема обработки и передачи сообщений.

ЗАКЛЮЧЕНИЕ

Анализ статистических данных показал, что стабильная работа большинства крупных телекоммуникационных и ИТ-прдеприятий зависит от бесперебойной работы их оборудования, а также от защищенности данных от искажения и потерь. В связи с этим, опираясь на рассмотренные в теоретической части диссертации стандарты, предприятия и операторы разрабатывают планы обеспечения непрерывности бизнеса. Для внедрения данных планов организуются отдельные структурные подразраздения высококлассных специалистов, в задачи которых входит разработка технических и организационных мероприятий по защите информации от потерь и искажений. В работе рассмотрены основные технологии защиты информации, методы восстановления данных, а также организационные меры по защите данных. Особое внимание уделено методам и средствам защиты информации, рассмотренным в разрезе их исторического развития.

В магистерской диссертации были рассмотрены существующие методы и средства обеспечения непрерывного функционирования ИТ-сервисов и систем в условиях чрезвычайных ситуаций. Была разработана схема межбанковского обмена конфиденциальной информацией разного типа с использованием защищенной сети. Данные передаются по сети в зашифрованном виде, сеть не имеет доступа в Интернет, безопасный стык с сетью обеспечивает наличие файервола. Сети банков соединяются с защищенной сетью посредством высокоскоростных оптоволоконных линий.

В работе было предложено использовать программное обеспечение белорусской разработки, которые может передавать различные виды сообщений с подтверждением доставки, а также использует шифрование и ЭЦП. Подлинность сертификатов обеспечивается функционированием в сети отдельного сервера с развернутым программным обеспечением удостоверяющего центра. Программное обеспечение средств криптозащиты предоставляет сертифицированный в РБ комплекс «Авест». Также в сети предусмотрен резервный сервер, на котором поддерживается актуальная база данных сообщений. Таким образом, разработанная сеть является защищенной и в ней обеспечивается резервирование 1+1 данной ИТ-услуги.

Для выполнения требований по скорости передачи информации в схеме предложено использовать высокопроизводительное оборудование компании Cisco.

В сети предусмотрено наличие центра сертификации открытых

Учитывая, что одной из составляющей программного комплекса является база данных передаваемых документов, которая организуется как на рабочем месте пользователя, так и на сервере СГДС с помощью MS SQL Server,

в работе в общем виде рассмотрен вариант репликации данных методом транзакций. ключей, что решает проблему подмены открытых ключей, а также осуществление процесса репликации данных и установка в сети резервного сервера для обеспечения надежности функционирования системы в случае непредвиденного сбоя сервера или возникновения чрезвычайной ситуации

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. Кемежук, М.М. Методы обеспечения надежности функционирования IT-систем в условиях чрезвычайной ситуации / М.М.Кемежук // Современные средства связи: материалы XVIII Международной науч.-техн. конф. / Высший государственный колледж связи. – Минск 2013 – с.169;

2. Кемежук, М.М Обеспечение пожарной безопасности высотных зданий / М.М.Кемежук // Материалы Международной научно-технической конференции 50 лет МРТИ-БГУИР, 18-19 марта 2014 г / Белорусский государственный университет информатики и радиоэлектроники – Минск 2014 – (сборник в печати);

3. Кемежук, М.М. Организационные меры по защите ит-сервисов в условиях чрезвычайной ситуации / М.М.Кемежук // Современные средства связи: материалы XIX Международной науч.-техн. конф. / Высший государственный колледж связи. – Минск 2014 – с..