Тип работы: Дипломная работа

Предмет: Информационные технологии

Введение

Стремительное развитие информационных и коммуникационных связано с необходимостью обмена большими массивами информации. Современное общество всецело зависит от информационных систем различного рода - от крупных информационных порталов банков и государственных служб до небольших прикладных систем, используемых в организациях. Большинство государственных услуг переводится в электронную форму, растет доля онлайн платежей, проводимых через банковские информационные системы. Таким образом, информационные ресурсы в настоящее время представляют собой высокоценный актив, обеспечение сохранности которого является залогом успешности функционирования организаций различного рода деятельности. Потери информации с высокой вероятностью могут приводить к простоям в работе сотрудников организаций, что приводит к прямым убыткам, связанным с потерями в клиентской базе, просрочкам в исполнении заказов и подготовке документов и др. В качестве объектов обрабатываемой информации выступают: финансовые данные, элементы коммерческой тайны, объекты, охраняемые законодательством об авторском праве, а также данные о личной жизни и состоянии здоровья людей. Утечки информации, содержащей коммерческую тайну, могут выступать в качестве причины прямых убытков, вплоть до возникновения угрозы функционированию предприятия. Известен ряд прецедентов, когда из-за утечек персональных данных злоумышленники получали возможность совершения неправомерных действий (получать кредиты, снятие наличных средств в банкоматах, кража денежных средств с счетов, находящихся в электронных кошельках). Таким образом, задача обеспечения защиты информации на сегодняшний день имеет особую актуальность.
Цель дипломной работы заключается в анализе системы защиты серверов компании.
Задачи работы:
- проведение анализа теоретических аспектов функционирования систем информационной безопасности;
- проведение анализа структуры АИС изучаемого предприятия;
- проведение анализа существующей системы информационной безопасности на предприятии;
- разработка мероприятий по совершенствованию системы защиты информации в условиях исследуемого предприятия.
Объект исследования: информационная система ООО "Топ Пойнт".
Предмет исследования: система защиты информации в информационной системе исследуемого предприятия.
Методы исследования: анализ литературных источников, нормативно-правовых актов и стандартов в области защиты информации, анализ технической документации по средствам защиты информации, анализ функционирования системы защиты от сетевых атак.

1.Аналитическая часть
1.1 Общая характеристика ООО "Топ Пойнт"

Объектом исследования в рамках данной работы является ООО "Топ Пойнт".
Профиль деятельности компании - производство оборудования для скалолазания. омпания TOP POINT - российский производитель скалодромов, зацепов для скалолазания и ледолазания, а также оборудования для оснащения спортивных зон и тренировочного процесса. TOP POINT - один из первых современных производителей скалодромов в России, где работают люди, влюбленные в скалолазание и желающие постоянно развивать этот замечательный вид спорта.
С момента основания, уже более 15-ти лет и по настоящее время, компания TOP POINT проектирует и производит по собственной сертифицированной технологии современные и интересные скалодромы любого уровня и назначения.
Основные задачи - развитие производства и совершенствование продукции. На своих производственных площадях мы разместили мастерские для работы с деревом, пластиком, композитами и металлом. Сегодня компания TOP POINT на высоком уровне создает первичные формы и макеты пространственных решений, опытные образцы, мелкие и крупные партии серийных изделий.
Огромный ассортимент зацепов и накладных рельефов собственного производства позволит без труда укомплектовать даже самые крупные скалодромы как для проведения соревнований среди любителей и профессионалов, так и для постановки трасс или свободного наполнения плоскостей скального тренажера общего назначения для проведения тренировок.

Информация, циркулирующая в системе ООО "Топ Пойнт", может предоставляться и обрабатываться как в автоматизированной, так и в неавтоматизированной форме.
Объектами защиты информации в информационной системе ООО "Топ Пойнт" могут выступать:
- персональные данные сотрудников;
- информация о текущей деятельности предприятия;
- разработки оборудования для скалолазания;
- инженерная документация на разработанные проекты;
- элементы коммерческой тайны;
- ключи электронной подписи.

1.2 Общая характеристика локальной сети ООО "Топ Пойнт"

В рамках данной работы проведен анализ системы защиты информации в Центре обработки данных корпоративной сети ООО "Топ Пойнт". Особенностью его использования является доступ к информационным ресурсам компании со стороны удаленных филиалов, либо со стороны клиентов, которым доступ предоставляется при заключении контрактов на обслуживание. Ресурсы серверного программного обеспечения используют виртуальную среду, так как программное обеспечение и формат баз данных достаточно разнороден, при этом закупка дополнительного программного обеспечения нецелесообразна. В качестве виртуальных машин используется ПО VMWare.
Архитектура центра обработки данных ООО "Топ Пойнт" предполагает наличие двух сетей сети: открытой и защищенной. В открытой сети находятся рабочие станции специалистов, имеющие выход в Интернет. Данные рабочие станции не предполагают работу с конфиденциальной информацией. В защищенной сети подключены рабочие станции, на которых хранится или обрабатывается конфиденциальная информация.

Рисунок 3 - Принципиальная схема компонент локальной сети ООО "Топ Пойнт"

Документооборот с контрагентами реализован с использованием следующих технологий:
- по факсу;
- по электронной почте;
- по защищенным каналам.
Защищенная сеть не имеет соединений с открытой сетью, что делает рабочие станции, входящие в данную сеть, абсолютно недосягаемыми для атак из внешней сети, при этом использование только данной технологии на дает стопроцентной гарантии защищенности сети.
Обслуживание автоматизированной системы производится сторонней фирмой, с которой заключен договор

подряда.
Технические характеристики
Таблица 4 - Технические характеристики сервера HP Proliant
Характеристика Значение
Процессор 4 x Intel Xeon-2.67GHz (667MHz,2x2MB L2 Cache),
Оперативная память 4 x 2048MB PC2-5300 667MHz DDR2 ECC DIMM Fully Buffered
HDD 4 x 1024 GB SATA
Дополнительно DVD/ RW

Таблица 5 - Технические характеристики рабочей станции специалиста IRUErgo 310
Характеристика Значение
Периферия Есть
Монитор Acer G226HQLHbd, 21,5’, 1920x1080 (16:9), 8мс, LED, 250 кд/м2
Описание ОфисныйПК
Процессор Intel (TM) Core i3
Память 2048Mb
HDD 320Гб 7200 об/мин 32 Мб
Оптический накопитель DVD-ROM + CD-RW (COMBO) 52/32/52+16
Видеосистема 64-128Mb integrated
FDD есть
Аудио AC97
LAN Есть
Размеры ~ 415 x 185 x 505мм

Технические характеристики принтера Samsung ML-3750 приведены в таблице 6.
Таблица 6 - Технические характеристики принтера Samsung ML-3750
Элементы Описание
Размеры Ширина x длина x высота 366 x 368 x 272,9 мм (14,40 x 14,48 x 10,74 дюйм.) без дополнительного лотка
Плотность бумаги Устройство с расходными материалами 10,28 кг
Уровень шума Режим готовности 26 дБ(A)
Режим печати 52 дБ(A)
Температура Эксплуатация от 10 до 32 °C
Хранение (в упаковке) от -20 до 40 °C

Относительная влажность Эксплуатация от 20 до 80 %
Хранение (в упаковке) от 10 до 90 %

Таблица 7 - Характеристики коммутатора cisco catalyst 2960
Наименование Catalyst 2960 Plus 24 Port LAN
Тип EthernetSwitch
Семейство Catalyst 2960
Ширина 17.5"
Высота 1.7"
Глубина 9.3"
NetworkTechnology 10Base-T 100/1000Base-T
Количество портов 24
FlashMemory 32 MB
EthernetTechnology FastEthernet
PowerSource PowerSupply
InputVoltage 110 V AC 220 V AC
Port/ExpansionSlotDetails 24 x Fast Ethernet Network 2 x Gigabit Ethernet Uplink 2 x Fast Ethernet Expansion Slot
TwistedPairCableStandard Category 5
AdditionalInformation LAN Base Image installed Entry-level enterprise-class intelligent services
LimitedWarranty Lifetime

Management Telnet Syslog Web browser CiscoWorks Remote SPAN SNMP v1, v2c, and v3 Command-line interface Cisco Network Assistant Switching Database Manager Cisco Service Assurance Agent IEEE 802.1p CoS IEEE 802.1Q VLAN RMON groups (history, statistics, alarms, and ev
MemoryTechnology DRAM
Number of Network (RJ-45) Ports 24
ProductLine Catalyst

Далее в ходе работы над проектом мной был проведен анализ программной архитектуры информационной системы ООО "Топ Пойнт".
В таблице 8 приведен перечень программных продуктов, используемых в технологии работы специалистов ООО "Топ Пойнт"
Таблица 8. Перечень программных продуктов, используемых в технологии работы специалистов ООО "Топ Пойнт"
Наименование задачи Технологическое решение Расположение
АРМ Документооборот Web-интерфейс Web-сервер ООО "Топ Пойнт"
Учет техники Тонкий клиент MS SQL Server
1С 8.2: Бухгалтерский Учет Тонкий клиент Сервер 1С:Предприятие
1С 8.2: Комплексная Тонкий клиент Сервер 1С:Предприятие
АРМ Учет кассовых аппаратов Тонкий клиент MS SQL Server
Учет договоров Тонкий клиент MS SQL Server
Сдача отчетности в ПФР spu_orb Рабочие станции специалистов по бухучету
SberSign Тонкий клиент Рабочие станции специалистов по бухучету

Таким образом, как показано в таблице 1.6, информационные ресурсы ООО "Топ Пойнт" включают в себя работу как с внутренними ресурсами, так и работу с информационными ресурсами сторонних организаций, что предполагает наличие дополнительных требований к системе информационной безопасности. Вопросы обеспечения информационной безопасности в корпоративной сети ООО "Топ Пойнт" курирует ИТ-отдел.
В рамках данной работы проведен анализ защищенности корпоративной сети ООО "Топ Пойнт". На рисунке 4 показана принципиальная схема корпоративной сети исследуемой организации. Защита корпоративной сети ООО "Топ Пойнт" осуществляется с использованием технологии VPN.
Рисунок 4 - Принципиальная схема корпоративной сети ООО "Топ Пойнт"
Технология VPN в условиях ООО "Топ Пойнт" использует стандарт IPSec и наиболее распространенные протоколы VPN. В рамках данной модели установка процесса взаимодействия маршрутизаторов заказчика производится с использованием WAN-сети сервис-провайдера. В данном случае со стороны провайдера не требуется настройки VPN, а функцией являются лишь предоставление своих незащищённых сетей для передачи трафика заказчика. Сети провайдеров используются только для инкапсуляции или наложенного (прозрачного) соединения VPN между площадками клиента (ООО "Топ Пойнт") [1].
Настройка VPN и маршрутизация трафика производится с использованием телекоммуникационных средств клиента. Для организации технологии корпоративной сети предприятия производится установка маршрутизаторов, обеспечивающих взаимодействие сети офисов с VPN-сетью. На маршрутизаторы производится установка программного обеспечения для построения защищённых VPN.
В рамках данного проекта для реализации VPN-соединения между офисами ООО "Топ Пойнт" будет использоваться ПО OpenVPN. Технология, используемая в данном программном продукте, основана на использовании SSL-стандарта для осуществления безопасных соединений через Интернет.
ПО OpenVPN обеспечивает безопасность соединений на основе 2-го и 3-го уровней OSI. При условии конфигурирования OpenVPN в режиме моста возможно обеспечение безопасных соединений на основе второго уровня OSI, в режиме маршрутизации - на основе третьего уровня. OpenVPN не позволяет осуществить доступ к сетям с использованием браузерных технологий, а также для его функционирования требуется установка клиентского ПО.
Модель VPN, реализованная в условиях ООО "Топ Пойнт", приведена на рис.5.

Рисунок 5 - Модель VPN, реализованная в условиях ООО "Топ Пойнт"

Настройка маршрутизатора производится в головном офисе ООО "Топ Пойнт" в качестве VPN-сервера, а маршрутизация удаленных офисов производится с использованием VPN-клиентов. Подключение

маршрутизаторов VPN-сервера и VPN-клиентов к Интернету производится через сети провайдера. Кроме того, к главному офису можно подключить ПК

Список использованных источников

1. ООО "Топ Пойнт". [Электронный ресурс]. Режим доступа: http://ipmce.ru/about
2. IDS – Snort. О программе. [Электронный ресурс]. Режим доступа: http://www.netconfig.ru/ready/snort/
3. Сетевая защита информации. [Электронный ресурс]. Режим доступа: http://ic-dv.ru/uslugi/sredstva_doverennoj_zagruzki/
4. Сетевые атаки и их виды. [Электронный ресурс]. режим доступа: https://www.kakprosto.ru/kak-848505-chto-takoe-setevaya-ataka
5. Блинов А.М. Информационная безопасность. – СПб: СПбГУЭФ, 2011 - 96с.
6. Андрианов В.В., Зефиров С.Л., Голованов В.Б., Голдуев Н.А. Обеспечение информационной безопасности бизнеса. – М.: Альпина Паблишерз, 2011 – 338с.
7. Стефанюк В.Л. Обеспечение физической защиты сетевых ресурсов. – М.: Наука, 2014. - 574 с.
8. Якубайтис Э.А. Информационные сети и системы: Справочная книга.- М.: Финансы и статистика, 2011. – 232с.
9. Разработка инфраструктуры сетевых служб Microsoft Windows Server 2008. Учебный курс MCSE М.: Взд-во Русская редакция, 2009.
10. Сосински Б., Дж. Московиц Дж. Windows 2008 Server за 24 часа. – М.: Издательский дом Вильямс, 2008.
11. Герасименко В.А., Малюк А.А. Основы защиты информации. – СПб.: Питер, 2010. – 320с
12. Гук М. Аппаратные средства локальных сетей. Энциклопедия. – СПб.: Питер, 2010. – 576с.
13. Иопа, Н. И. Информатика: (для технических специальностей): учебное пособие– Москва: КноРус, 2011. – 469 с.
14. Акулов, О. А., Медведев, Н. В. Информатика. Базовый курс: учебник – Москва: Омега-Л, 2010. – 557 с.
15. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия Интернет-университет информационных технологий - ИНТУИТ.ру, 2012
16. МогилевА.В.. Информатика: Учебное пособие для вузов - М.: Изд. центр "Академия", 2011
17. Партыка Т.Л. Операционные системы и оболочки. - М.: Форум, 2011
18. Под ред. проф. Н.В. Макаровой: Информатика и ИКТ. - СПб.: Питер, 2011
19. Новиков Ю. В., Кондратенко С. В. Основы локальных сетей. КуПК лекций. – СПб.:Интуит, 2012. – 360с.
20. Ташков П.А. Защита компьютера на 100%. - СПб.: Питер, 2011
21. Самоучитель Microsoft Windows XP. Все об использовании и настройках. Изд. 2-е, перераб. и доп. М. Д. Матвеев, М. В. Юдин, А.В. Куприянова. Под ред. М. В. Финкова.– СПб.: Наука и Техника, 2011. – 624 с.: ил.
22. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. – М.: Академия, 2011. – 256 с.