Анализ информационных ресурсов и выработка концептуальных основ деятельности по обеспечению корпоративной информационной безопасности для ООО “Т-СЕРВИС ЛОГИСТИКС”

Наименование компании: Общество с Ограниченной Ответственностью «Т-СЕРВИС ЛОГИСТИКС»

Веб-сайт: [www.t-slog.ru](http://www.t-slog.ru)

Описание деятельности компании:

Компания "Т-СЕРВИС ЛОГИСТИКС" находится на российском рынке транспортно-логистических услуг с 2007 года.

С 2007 по 2015гг. организация занималась следующими направлениями деятельности:

1. Организация перевозок грузов
2. Деятельность агентов по оптовой торговле топливом, рудами, металлами и химическими веществами
3. Оптовая торговля прочими непродовольственными потребительскими товарами
4. Маркетинговые исследования и выявление общественного мнения
5. Консультирование по вопросам коммерческой деятельности и управления
6. Рекламная деятельность

Функциональная блок-схема компании

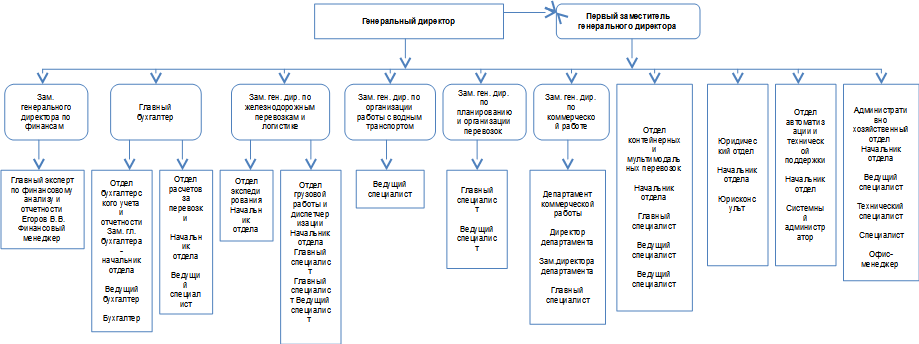
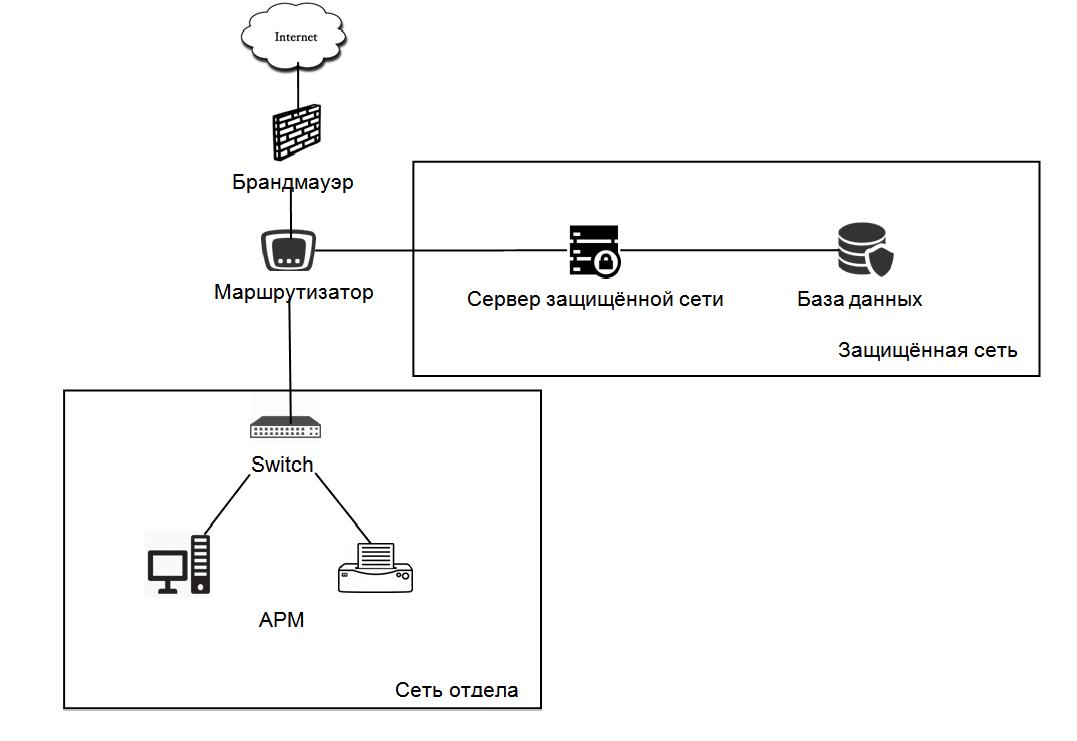


Схема архитектуры ИТ-сети компании



Определение номенклатуры информационных активов

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Вид актива** | **Наименование актива** | **Владелец** | **Степень важности** | **Угрозы** | **Уязвимости** | **Обоснование выбранной степени важности** |
| база данных 1С: Бухгалтерия | база данных сотрудников и расчёта заработной платы | отдел бух.учёта и отчётности, отдел расчётов за перевозки | высокая(⅘) | инсайдерская утечка данных, взлом сервера базы данных | возможность отследить входящий/исходящий трафик | без базы данных сотрудников и расчёта заработной платы, предприятие может функционировать |
| системная документация | документация содержит определенную важную информацию, описания процессов работы бизнес-приложений, процедур, структур данных, процессов авторизации | все отделы | средняя(⅗) | инсайдерская утечка данных, взлом файловогосервера | взлом доступа | нарушения доступа и утечка описания бизнес-процессов не являются критичными для функционирования предприятия |
| оперативные данные | данные по дислоцированию грузопередач | отдел грузовой работы и диспетчеризации, отдел контейнерных и мультимодальных перевозок | средняя(⅗) | инсайдерская утечка данных, взлом подсети отдела | авторизация | нарушения работы в пределах отдела, локальная утечка |
| база данных 1С: Предприятие | база юридической документации | юридический отдел, отдел экспедирования | средняя (3/5) | инсайдерская утечка данных, взлом сервера базы данных | взлом доступа | утечка юридической документации может быть использована против компании, но непосредственной угрозы нет |

Определение видов и номенклатуры тайн

|  |  |  |
| --- | --- | --- |
| **Вид (разновидность) тайны** | **Содержание сведений, составляющих тайну** | **Численность пользователей(П), рабочих мест(РМ), филиалов(Ф), вовлечённых в обработку КИ** |
| Персональные данные | Сведения о сотрудниках | бухгалтерия - 3П, 2РМ  юридический отдел - 2П, 2РМ |
| Коммерческие данные | Данные организации | департамент коммерческой работы - 3П, 3РМ |
| Сведения о результатах проведенной оценки уязвимости объектов транспортной инфраструктуры и транспортных средств | Данные транспортных инфраструктуры и средств | отдел экспедирования - 1П, 1РМ  отдел грузовой работы - 4П, 4РМ  отдел контейнерных и мультимодальных перевозок - 4П, 4РМ |

Перечень сведений, составляющих коммерческую тайну организации.

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Общие группы сведений, составляющих тайну** | **Перечень конкретных сведений, входящих в состав группы** | **Сотрудники каких подразделений допущены к данным сведениям** |
| 1 | структура кадров и производства | База данных 1С | бухгалтерия |
| 2 | условия контрактов, включая цены | данные организации, системная документация | юридический отдел  департамент коммерческой работы |
| 3 | сведения об условиях фрахтования транспорта иностранных компаний и фирм под перевозку внешнеторговых грузов | оперативные данные | отдел экспедирования  отдел грузовой работы  отдел контейнерных и мультимодальных перевозок |
| 4 | Сведения о структуре, составе, материально-техническом оснащении службы безопасности предприятия | локальная база данных | административно-хозяйственный отдел  отдел автоматизации и техподдержки |

Наиболее важные дестабилизирующие факторы (ДФ), формирующие угрозы информационной безопасности

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Вид и разновидность тайны** | **В состав какого информационного актива входят соответствующие данные** | **Наиболее значимые ДФ для каждого пункта**  **(по мере убывания важности)** | **На каких носителях распространяются соответствующие данные** |
| 1 | Персональные данные, Сведения о структуре, составе, материально-техническом оснащении предприятия | База 1С, локальные базы данных (AD/LDAP) | Халатность сотрудников, недостаточная защита от внешних угроз, ненадёжность носителя | Серверные хранилища данных |
| 2 | Коммерческие данные, условия контрактов, цены | Данные организации, системная документация, юридические документы | Инсайдерство, недостаточная защита от внешних угроз | Серверные хранилища данных, бумажный носитель |
| 3 | Сведения о результатах проведенной оценки уязвимости объектов транспортной инфраструктуры и транспортных средств,  сведения об условиях фрахтования транспорта иностранных компаний и фирм под перевозку внешнеторговых грузов | Оперативные данные, системная документация, инструкции | Инсайдерство, недостаточная защита от внешних угроз | Серверные хранилища данных, бумажный носитель |

Наибольшая угроза для сведений, составляющих тайны и информационных активов, включающих соответствующие данные

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Вид и разновидность тайны** | **В состав какого информационного актива входят соответствующие данные** | **Условия разведывательного контакта** | **Методы доступа к добываемой информации** | **Способы дистанционного добывания** |
| 1 | Персональные данные, Сведения о структуре, составе, материально-техническом оснащении предприятия | База 1С, локальные базы данных (AD/LDAP) | Возможность копирования данных, утечка носителей, удалённый доступ | Копирование данных на носитель | Перехват трафика, взлом шифрования, разбор пакетов данных |
| 2 | Коммерческие данные, условия контрактов, цены | Данные организации, системная документация, юридические документы | Возможность копирования данных, утечка оригиналов | Копирование данных на носитель, доступ к документам | Перехват трафика, взлом шифрования, разбор пакетов данных для данных в цифровом виде,  средства наблюдения |
| 3 | Сведения о результатах проведенной оценки уязвимости объектов транспортной инфраструктуры и транспортных средств,  сведения об условиях фрахтования транспорта иностранных компаний и фирм под перевозку внешнеторговых грузов | Оперативные данные, системная документация, инструкции | Возможность копирования данных, утечка оригиналов | Копирование данных на носитель, доступ к документам | Перехват трафика, взлом шифрования, разбор пакетов данных для данных в цифровом виде, средства наблюдения |

Распределение информационных активов, содержащих сведения, составляющие тайны, по зонам доступа

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Информационные активы** | **Какие виды и разновидности тайн содержат** | **В какой зоне**  **должны находиться** |
| 1 | База 1С, локальные базы данных (AD/LDAP) | Персональные данные, Сведения о структуре, составе, материально-техническом оснащении предприятия | Защищённая сеть, разграничение прав доступа, отсутствие физического доступа |
| 2 | Данные организации, системная документация, юридические документы | Коммерческие данные, условия контрактов, цены | Защищённая сеть, разграничение прав доступа, отсутствие физического доступа, сейфы, секретные комнаты |
| 3 | Оперативные данные, системная документация, инструкции | Сведения о результатах проведенной оценки уязвимости объектов транспортной инфраструктуры и транспортных средств,  сведения об условиях фрахтования транспорта иностранных компаний и фирм под перевозку внешнеторговых грузов | Защищённая сеть, разграничение прав доступа, отсутствие физического доступа, сейфы, секретные комнаты, защищённые и помехоустойчивые каналы связи |

Наиболее опасные каналы утечки информации, способы и средства противодействия утечке

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Информационные активы** | **Наиболее опасные каналы утечки для каждого актива** | **Способ противодействия утечке** | **Средство противодействия утечке** |
| 1 | База 1С, локальные базы данных (AD/LDAP) | Инсайдерская утечка (копирование) | Правовой и технический | Разграничение прав доступа, правовые акты |
| 2 | Данные организации, системная документация, юридические документы | Инсайдерская утечка (копирование или кража оригинала) | Правовой и технический | Разграничение прав доступа, правовые акты |
| 3 | Оперативные данные, системная документация, инструкции | Инсайдерская утечка, перехват каналов связи | Правовой и технический | Разграничение прав доступа, криптография, правовые акты |