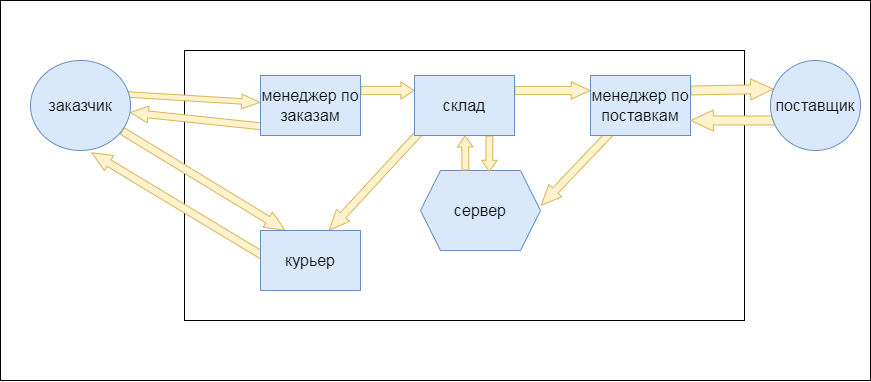
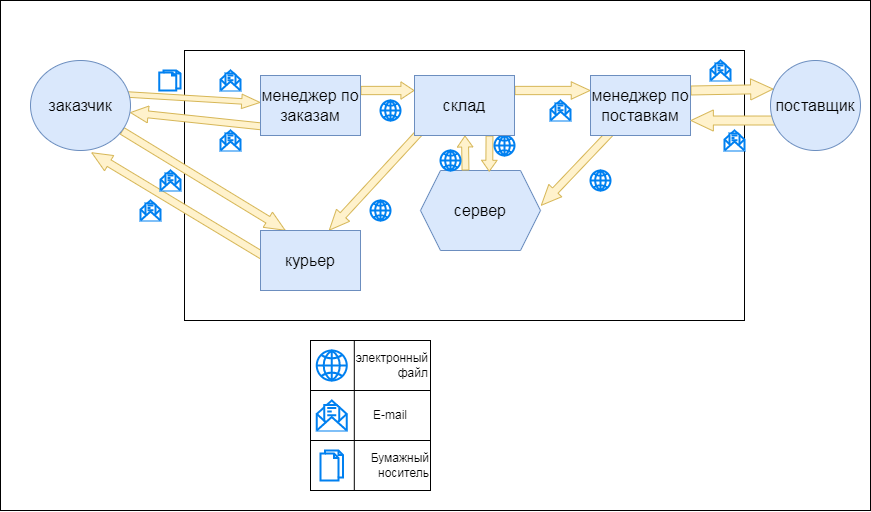
1. **Выбор объекта информатизации и его компонент**
   1. Объект информации – магазин компьютерной техники.
   2. Первым этапом будет обращение заказчика менеджеру заказов, далее заказчику поступает подтверждение заказа(с полным описание) на почту.
   3. После подтверждения заказа информация передается на склад.
      1. Далее если все компоненты заказа присутствуют на складе, склад передает информацию о заказе на сервер, а потом курьеру.
      2. Если не все компоненты заказа находятся на складе, тогда склад передает запрос на закупку товара менеджеру по закупкам.
      3. Менеджер по закупкам передает запрос поставщикам.
      4. Поставщики передают информацию о поставке менеджеру по поставкам.
      5. Менеджер по поставкам передают информацию о поставке серверу.
      6. Далее сервер передает информацию на склад.
   4. После сборки заказа, информация о нем будет передана курьеру.
   5. Когда курьер получит заказ он уведомит об этом заказчика и выберет удобное время для доставки.



1. **Определение способов передачи данных для всех потоков информации.**

****

1. **Определение свойств информации, которые необходимо обеспечить**.

Таблица 2

| Номер потока | Назначение  информационных  потоков | Конфиденциальность | Целостность | Доступность |
| --- | --- | --- | --- | --- |
| 1 | Заказчик -> менеджер  по заказам | Да (Так как заказ является коммерческой тайной) | Нет (Так как при поступлении запроса менеджеру по продажам, информация может поменяться) | Нет (Наша компания не может обеспечить доступность информации, так как это зависит только от заказчика) |
| 2 | Менеджер по продажам -> заказчик | Да (Так как заказ является коммерческой тайной) | Да | Да (Заказчик может запросить повторную отправку данных о заказе) |
| 3 | Менеджер по продажам -> склад | Да (Так как заказ является коммерческой тайной) | Да (Работники склада получат информацию, которую указал менеджер по заказам) | Да (Работники склада могут в любой момент запросить текущую информацию о заказе) |
| 4 | Склад -> менеджер по поставкам | Да (Так как заказ является коммерческой тайной) | Да (Менеджер по поставкам получит информацию указанную непосредственно работниками склада) | Да (Менеджер по поставкам в любое время может уточнить информацию у работников склада) |
| 5 | Менеджер по поставкам -> поставщик | Да (Так как заказ является коммерческой тайной) | Да (Поставщик получат информацию указанную непосредственно менеджером по продажам) | Да (Поставщик в любое время может уточнить информацию у менеджера по закупкам) |
| 6 | Поставщик -> менеджер по поставкам | Да (Так как заказ является коммерческой тайной) | Нет (Наша компания не может гарантировать целостность, она должна обеспечиваться на стороне поставщика) | Нет (Наша компания не может обеспечить доступность, она должна быть обеспечена на стороне поставщика) |
| 7 | Менеджер по поставкам -> сервер | Да (Так как заказ является коммерческой тайной) | Да (На сервер выгружается та информация, которую занес менеджер по поставкам) | Да (Менеджер по заказам в любой момент может обновить информацию на сервере) |
| 8 | Сервер -> склад | Да (Так как заказ является коммерческой тайной) | Да (На сервере находится та информация о поставке, которую занес менеджер по поставкам) | Да (Работники склада в любой момент могут подать запрос на сервер, чтобы уточнить информацию) |
| 9 | Склад -> сервер | Да (Так как заказ является коммерческой тайной) | Да (Работники склада выгружают на сервер актуальную информацию о заказе) | Да (Работники в любое время могут подать запрос, на обновление информации хранящийся на сервере) |
| 10 | Склад -> курьер | Да (Так как заказ является коммерческой тайной) | Да (Курьер получает указанную информацию непосредственно работниками склада) | Да (Курьер в любой момент может уточнить информацию у работников склада) |
| 11 | Курьер -> заказчик | Да (Так как заказ является коммерческой тайной) | Да (Заказчик получает указанную информацию непосредственно курьером) | Да (Заказчик в любой момент может уточнить информацию у курьера) |
| 12 | Заказчик -> курьер | Да (Так как заказ является коммерческой тайной) | Нет (Наша компания не может гарантировать целостность информации предоставленной заказчиком (например, данные о встрече могут поменяться)) | Нет (Наша компания не может обеспечить доступность информации, так как это зависит только от заказчика (например, уточнение даты и время)) |

Таблица 3

| Номер потока | Способ передачи  информации | Назначение  информационных  потоков | Св-ва информации,  которые необходимо  обеспечить  (К – Конфиденциальность, Ц – целостность, Д - Доступность) |
| --- | --- | --- | --- |
| 1 | E-mail, Бумажный носитель | Заказчик -> менеджер  по заказам | К |
| 2 | E-mail | Менеджер по продажам -> заказчик | К, Ц, Д |
| 3 | Электронный файл | Менеджер по продажам -> склад | К, Ц, Д |
| 4 | E-mail | Склад -> менеджер по поставкам | К, Ц, Д |
| 5 | E-mail | Менеджер по поставкам -> поставщик | К, Ц, Д |
| 6 | E-mail | Поставщик -> менеджер по поставкам | К |
| 7 | Электронный файл | Менеджер по поставкам -> сервер | К, Ц, Д |
| 8 | Электронный файл | Сервер ->  склад | К, Ц, Д |
| 9 | Электронный файл | Склад ->  сервер | К, Ц, Д |
| 10 | Электронный файл | Склад ->  курьер | К, Ц, Д |
| 11 | E-mail | Курьер -> заказчик | К, Ц, Д |
| 12 | E-mail | Заказчик -> курьер | К |

1. **Определение возможных негативных последствий от реализации угроз безопасности информации**

Таблица 4

| Номер | Виды риска (ущерба) | Возможные негативные последствия |
| --- | --- | --- |
| У1 | Ущерб физическому лицу. | * Нарушение неприкосновенности частной жизни. * Нарушение личной, семейной тайны, утрата чести и доброго имени. * Нарушение тайны переписки, телефонных переговоров, иных сообщений. * Нарушение конфиденциальности (утечка) персональных данных. * Разглашение персональных данных граждан. |
| У2 | Нанесение ущерба юридическому лицу. | * Недополучение ожидаемой (прогнозируемой) прибыли. * Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. * Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств). * Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса * Срыв запланированной сделки с партнером. * Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. * Потеря клиентов, поставщиков. * Потеря конкурентного преимущества. * Невозможность заключения договоров, соглашений. * Нарушение деловой репутации. * Снижение престижа. * Утрата доверия. * Причинение имущественного ущерба * Неспособность выполнения договорных обязательств. * Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций). * Принятие неправильных решений. * Публикация недостоверной информации на веб-ресурсах организации. * Использование веб-ресурсов для распространения и управления вредоносным программным обеспечением. * Рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени. * Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.) |

1. **Определение объектов воздействия и видов воздействия на них.**

Таблица 5

| Негативные последствия | Объекты воздействия | Виды воздействия |
| --- | --- | --- |
| Разглашение персональных данных граждан. (У1) | База данных информационной системы, содержащая идентификационную информацию граждан. | Утечка идентификационной информации граждан из базы данных. |
| Веб-приложение информационной системы, обрабатывающей идентификационную информацию граждан. | Несанкционированный доступ к идентификационной информации граждан, содержащейся в веб-приложении информационной системы. |
| Срыв запланированной сделки с партнером. (У2) | АРМ руководителя организации. | Модификация информации и отправка электронных писем с недостоверной информацией от имени руководителя организации. |
| Электронный почтовый ящик руководителя организации. | Модификация информации и отправка электронных писем с недостоверной информацией от имени руководителя организации. |
| Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.) (У2) | АРМ оператора. | Несанкционированный доступ или хищение конфиденциальной информации содержащей личные данные заказчиков. |
| АРМ руководителя организации. | Несанкционированный доступ или хищение конфиденциальной информации содержащей личные данные работников. |
| Принятие неправильных решений. (У2) | Почта руководителя отдела логистики(склад). | Модификация информации и отправка электронных писем с недостоверной информацией от имени руководителя отдела. |
| Почта менеджера по закупкам. | Модификация информации и отправка электронных писем с недостоверной информацией от имени менеджера. |
| Почта менеджера по заказам. | Модификация информации и отправка электронных писем с недостоверной информацией от имени менеджера. |
| Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств). (У2) | Почта менеджера по закупкам. | Модификация информации и отправка электронных писем с недостоверной информацией от имени менеджера. |
| АРМ руководителя отдела логистики(склад). | Модификация информации от имени руководителя отдела. |

1. **Определение источников угроз безопасности информации**

Таблица 6

| Виды нарушителей | Возможные цели реализации угроз безопасности информации | | | Соответствие целей видам риска (ущерба) и возможным негативным последствиям |
| --- | --- | --- | --- | --- |
| Нанесение ущерба физическому лицу | Нанесение ущерба  юридическому  лицу,  индивидуальному  предпринимателю | Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности |
| Специальные службы иностранных государств | - | - | - | - |
| Террористические, экстремистские группировки | - | - | - | - |
| Преступные группы (криминальные структуры) | +  (получение финансовой выгоды за счет кражи и продажи персональных данных граждан) | +  (желание само реализоваться) | - | У1 (нарушение конфиденциальности персональных данных граждан) У2 (нарушение деловой репутации) |
| Отдельные физические лица (хакеры) | +  (получение финансовой выгоды за счет кражи и продажи персональных данных граждан, желание само реализоваться) | +  (Получение финансовой выгоды за счет несанкционированного доступа к конфиденциальной информации) | - | У1 (нарушение конфиденциальности персональных данных граждан)  У2 (Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)) |
| Конкурирующие организации | - | +  (Получение конкурентных преимуществ) | - | У2 (Потеря конкурентного преимущества.) |
| Разработчики программных, программноаппаратных средств | - | +  (передача информации о юридическом лице третьим лицам) | - | У2 (недополучение ожидаемой прибыли) |
| Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем | - | - | - | - |
| Поставщики вычислительных услуг, услуг связи | - | - | - | - |
| Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ | - | - | - | - |
| Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) | - | - | - | - |
| Авторизованные пользователи систем и сетей | +  (непреднамеренные, неосторожные или неквалифицированные действия) | - | - | У1 (финансовый, иной материальный ущерб физическим лицам) |
| Системные администраторы и администраторы безопасности | +  (получение финансовой выгоды за счет кражи и продажи персональных данных граждан) | +  (Получение финансовой выгоды за счет несанкционированного доступа к конфиденциальной информации) | - | У1 (финансовый, иной материальный ущерб физическим лицам)  У2 (Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)) |
| Бывшие (уволенные) работники (пользователи) | +  (Получение финансовой или иной материальной выгоды) | +  (Месть за ранее совершенные действия) | - | У1 (финансовый, иной материальный ущерб физическим лицам)  У2 (Принятие неправильных решений.  ) |

Таблица 7

| Номер | Виды риска (ущерба) и возможные негативные последствия | Виды актуального нарушителя | Категория нарушителя | Уровень возможностей нарушителя |
| --- | --- | --- | --- | --- |
| 1 | У1:  Нарушение конфиденциальности персональных данных граждан, финансовый, иной материальный ущерб физическим лицам | Преступные группы (криминальные структуры) | Внешний |  |
| Отдельные физические лица (хакеры) | Внешний |  |
| Авторизованные пользователи систем и сетей | Внутренний |  |
| Системные администраторы и администраторы безопасности | Внутренний |  |
| Бывшие (уволенные) работники (пользователи) | Внутренний |  |
| 2 | У2:  нарушение деловой репутации, утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.), Потеря конкурентного преимущества, недополучение ожидаемой прибыли, Принятие неправильных решений. | Преступные группы (криминальные структуры) | Внешний |  |
| Отдельные физические лица (хакеры) | Внешний |  |
| Конкурирующие организации | Внешний |  |
| Разработчики программных, программноаппаратных средств | Внутренний |  |
| Системные администраторы и администраторы безопасности | Внутренний |  |
| Бывшие (уволенные) работники (пользователи) | Внутренний |  |
| 3 | У3:  - | - | - | - |

1. **Определение способов реализации (возникновения) угроз безопасности информации**

Таблица 8

| номер | Виды нарушителя | Категория нарушителя | Объект воздействия | Доступные интерфейсы | Способы реализации |
| --- | --- | --- | --- | --- | --- |
| 1 | Специальные службы иностранных государств | **-** | **-** | **-** | **-** |
| 2 | Террористические, экстремистские группировки | **-** | **-** | **-** | **-** |
| 3 | Преступные группы (криминальные структуры) | Внешний | БД менеджера заказов хранящую конфиденциальную информацию о заказчиках | Веб-интерфейс удаленного администрирования базы данных информационной системы | Несанкционированный доступ к базе данных |
| БД курьера хранящую конфиденциальную информацию о возможных адресах заказчиков | Веб-интерфейс удаленного администрирования базы данных информационной системы | Несанкционированный доступ к базе данных |
| БД сервера хранящего коммерческую информацию | Веб-интерфейс удаленного администрирования базы данных информационной системы | Несанкционированный доступ к базе данных |
| 4 | Отдельные физические лица (хакеры) | Внешний | Линия связи между менеджером по заказам и сервером(локальная сеть) | Канал передачи данных между сервером и бухгалтерией | Внедрение вредоносного программного обеспечения |
| Линия связи между менеджером по поставкам и сервером(локальная сеть) | Канал передачи данных между сервером и бухгалтерией | Использование ошибок ПО организации |
| Сервер | Удаленный канал управления | Использование ошибок ПО организации |
| 5 | Конкурирующие организации | Внешний | Линия связи между менеджером по заказам и складом(локальная сеть) | АРМ менеджера | Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя |
| 6 | Разработчики программных, программноаппаратных средств | Внутренний | БД менеджера заказов хранящую конфиденциальную информацию о заказчиках | Съемные машинные носители информации, подключаемые к АРМ пользователя | Уязвимость при разработке приложения |
|  | БД курьера хранящую конфиденциальную информацию о возможных адресах заказчиков | Съемные машинные носители информации, подключаемые к АРМ пользователя | Уязвимость при разработке приложения |
| 7 | Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем | **-** | **-** | **-** | **-** |
| 8 | Поставщики вычислительных услуг, услуг связи | **-** | **-** | **-** | **-** |
| 9 | Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ | **-** | **-** | **-** | **-** |
| 10 | Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) | **-** | **-** | **-** | **-** |
| 11 | Системные администраторы и администраторы безопасности | Внутренний | БД менеджера по заказам хранящую конфиденциальную информацию заказчиках | Веб-интерфейс удаленного администрирования базы данных информационной системы | Использование ошибок ПО организации |
| 12 | Бывшие (уволенные) работники (пользователи) | Внутренний | БД курьера хранящую конфиденциальную информацию о возможных адресах заказчиков | Веб-интерфейс удаленного администрирования базы данных информационной системы | Доступ к АРМ пользователя |

1. **Определение угроз безопасности информации**

УБИi =[нарушитель (источник угрозы); объекты воздействия; способы реализации угрозы; негативные последствия;]

УБИ1 =[ Преступные группы; БД менеджера заказов; использование ошибок ПО организации; продажа конфиденциальной информации о заказчике;].

УБИ2 =[ Преступные группы; БД курьеров; использование ошибок ПО организации; получение конфиденциальной информации о клиентах;]

УБИ3 =[ Преступные группы; БД сервера организации; использование ошибок ПО организации; несанкционированный доступ к БД организации;]

УБИ4 =[ хакерская группировка; Линия связи между менеджером по заказам и сервером; рассылка сообщений по почте; Внедрение вредоносного программного обеспечения;]

УБИ5 =[ хакерская группировка; Линия связи между менеджером по поставкам и сервером; использование ошибок ПО организации; использование конфиденциальной информации о клиентах в личных целях;]

УБИ6 =[хакерская группировка; сервер; использование ошибок ПО организации; модификация БД организации;]

УБИ7 =[ сотрудник, которого подкупила конкурирующая организация; Линия связи между менеджером по заказам и складом; вредоносное ПО установленное на внешнем носителе; Потеря конкурентного преимущества;]

УБИ8 =[ Разработчики программных, программноаппаратных средств; БД менеджера заказов хранящую конфиденциальную информацию о заказчиках; ошибка в написании кода; возможность модификации конфиденциальной информации;]

УБИ9 =[ Разработчики программных, программноаппаратных средств; БД курьера хранящую конфиденциальную информацию о возможных адресах заказчиков; ошибка в написании кода; утечка конфиденциальной информации;]

УБИ10 =[ Системные администраторы и администраторы безопасности; БД менеджера по заказам хранящую конфиденциальную информацию заказчиках; Использование ошибок ПО организации; продажа конфиденциальных данных о клиентах;]

УБИ11 =[ Бывшие (уволенные) работники (пользователи); БД курьера хранящую конфиденциальную информацию о возможных адресах заказчиков; доступ к АРМ пользователя информации ; разрушение репутации компании;]