БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

**Лабораторная работа №1**

**«**Разработка и внедрение политики безопасности логистической компании»

Выполнила:

студентка 3 курса 5 группы

Почиковская Юлия Сергеевна

Вариант 10

Проверил:

Берников В. О.

Минск 2022

**Содержание**

[1. Введение 3](#_Toc95806233)

[2. Обоснование актуальности, цели и задачи разработки ПИБ. 4](#_Toc95806234)

[3. Объекты защиты. 6](#_Toc95806235)

[4. Основные угрозы и их источники 8](#_Toc95806236)

[5. Оценка угроз, рисков и уязвимостей 10](#_Toc95806237)

[6. Методы, меры и средства обеспечения требуемого уровня защиты информационных ресурсов. 11](#_Toc95806238)

[7. Вывод 13](#_Toc95806239)

1. **Введение**

Защита информации от утечки в логистических компаниях играет значительную роль в первую очередь из-за значительных экономических рисков, заложенных в данной отрасли. К тому же, согласно законодательству транспортные компании, занимающиеся пассажирскими перевозками, должны обеспечивать всестороннюю защиту и предоставлять гарантии такой защиты своим клиентам.

Применение политики безопасности в логистических компаниях во многом обусловлено высокой ценностью данных, используемых в таких организациях. Клиентские базы, расценки, сведения о работниках — все это и многое другое должно оставаться в пределах компании и ее корпоративной сети. Более того, такие компании оперируют большими объемами информации о маршрутах и перевозимых грузах. Такие данные могут заинтересовать как конкурентов, так и преступные группировки. Эти риски делают необходимым обеспечение информационной безопасности организации.

Политика ИБ необходима для обоснования введения защитных мер в компании. Политика должна быть утверждена высшим административным органом компании (генеральный директор, совет директоров и т.п.).

1. **Обоснование актуальности, цели и задачи разработки ПИБ.**

Информационная безопасность – все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности информации или средств ее обработки.

Целостность информационных данных означает способность информации сохранять изначальный вид и структуру как в процессе хранения, как и после неоднократной передачи. Вносить изменения, удалять или дополнять информацию вправе только владелец или пользователь с легальным доступом к данным.

Конфиденциальность – характеристика, которая указывает на необходимость ограничить доступа к информационным ресурсам для определенного круга лиц. В процессе действий и операций информация становится доступной только пользователям, который включены в информационные системы и успешно прошли идентификацию.

Доступность информационных ресурсов означает, что информация, которая находится в свободном доступе, должна предоставляться полноправным пользователям ресурсов своевременно и беспрепятственно.

Достоверность указывает на принадлежность информации доверенному лицу или владельцу, который одновременно выступает в роли источника информации.

Политика компании в области информационной безопасности предусматривает принятие необходимых мер в целях защиты ресурсов от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в логистической компании.

В компании информация существует и передается в различных формах: на бумажном носителе, в электронном виде при хранении на носителе, передается по почте или с использованием электронных устройств, передаваться устно в процессе общения. Информация должна быть защищена независимо от ее формы и способа ее распространения, передачи и хранения.

Главные цели компании не могут быть достигнуты без своевременного и полного обеспечения сотрудников информацией, необходимой им для выполнения своих служебных обязанностей.

Ответственность за соблюдение информационной безопасности несет каждый сотрудник компании.

Целью политики является создание условий, позволяющих предотвратить или минимизировать ущерб, который может быть нанесен в результате несанкционированного доступа, хищения служебной информации или нанесения ущерб техническим средствам обработки, хранения и передачи защищаемой информации.

Значимость обеспечения ИБ определяется наличием в общей системе информационных потоков предприятия сведений, составляющих не только коммерческую, но и государственную тайну, а также другие виды конфиденциальной информации: сведения, составляющие банковскую тайну, различные виды персональных данных, в т. ч. – врачебную тайну, интеллектуальную собственность компаний-партнеров и т. п.

Рекомендации по обеспечению безопасности информации:

* определить права и обязанности пользователей;
* коммерческая тайна самой логистической компании, данные о ее договорах, финансовых взаимоотношениях, бухгалтерская информация;
* коммерческая тайна клиентов и партнеров организации, данные об их активах, имуществе, платежах, произошедших страховых событиях;
* персональные данные сотрудников компании и сотрудников клиентов, эта информация иногда включает номера автомобилей, водительских удостоверений, кредитных карт;
* 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.

Руководители отделов компании должны обеспечить регулярный контроль за соблюдением положений политики безопасности, организовать периодические проверки соблюдения информационной безопасности с последующим представлением ежегодного отчета по результатам указанной проверки руководству.

1. **Объекты защиты.**

Логистическая компания - это предприятие, оказывающее услуги по транспортировке, обработке и хранению грузов, содействуя своим клиентам в процессе продвижения товаров от производителя к потребителю.

**Субъекты защиты:**

* Базы данных клиентов и вся интеллектуальная собственность сервиса;
* Носители информации, на которых зафиксированы, отображены защищаемые сведения;
* Личные дела сотрудников;
* Обращения к услугам компании физических лиц, журналы, ведомости, положения, инструкции, соглашения и обязательства о неразглашении, распоряжения, договоры, отчеты;
* Локальная сеть;
* Ключевая, парольная аутентифицирующая информацию;
* Финансовые данные компании

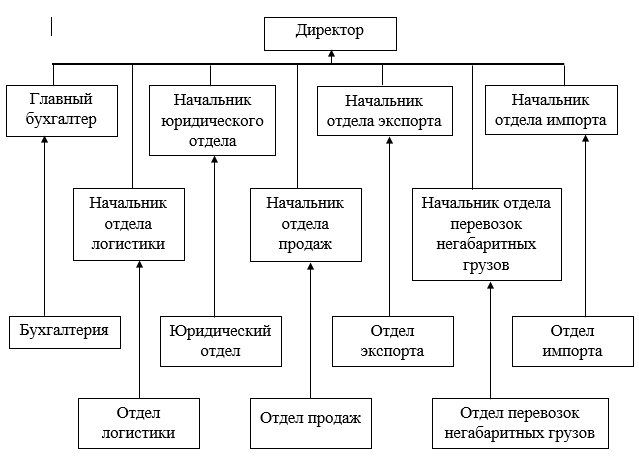
**Структура логистической компании:**

Рисунок 1. – Структура логистической компании

**Объекты защиты:**

* Работники компании (весь персонал и сотрудники компании всех уровней)
* Компании партнеры (компании, сотрудничество с которыми необходимо для организации деятельности компании)
* Клиенты компании

Информация, нуждающаяся в защите, хранится как в электронном, так и в бумажном виде на серверах компании, на персональных компьютерах сотрудников отделов и в архиве документов; с информацией работают сотрудники указанных отделов, и, соответственно, только сотрудники отделов имеют доступ к соответствующей информации.

Во главе компании стоит директор. Директор имеет полный доступ ко всей информации и ресурсам компании. Непосредственно директору подчиняются главный бухгалтер, начальник отдела логистики, начальник юридического отдела, начальник отдела продаж, начальник отдела экспорта, начальник отдела перевозок, начальник отдела импорта.

Наибольшую опасность несет собой директор, потому что у него имеется вся информация о логистической компании в целом и предоставляется различными отделами данной компании.

Бухгалтер имеет доступ к доходам и расходам денежных средств, и отвечает за начисление заработной платы каждому сотруднику и в случае утечки конфиденциальной информации и несанкционированном доступе к аккаунтам и информации, может быть нарушена финансовая сторона компании.

Менеджер по продажам имеет доступ к личным данным клиентов их счетам, адресам и в случае утечки данной информации пострадает не только сама компания, но и ее клиенты.

Из данной структуры следует выделить, что основную угрозу несёт директор и программисты в каждом отделе, так как они имеют наиболее высокий доступ к информации.

1. **Основные угрозы и их источники**

Угрозами безопасности информации являются:

* хищение (копирование) информации;
* уничтожение информации;
* модификация (искажение) информации;
* нарушение доступности (блокирование) информации;
* отрицание подлинности информации;
* навязывание ложной информации.

Носителями угроз безопасности информации являются источники угроз. В качестве источников угроз могут выступать как субъекты, так и объективные проявления. Причем, источники угроз могут находиться как внутри защищаемой организации - внутренние источники, так и вне ее - внешние источники.

Все источники угроз безопасности информации можно разделить на три основные группы:

* Обусловленные действиями субъекта (антропогенные источники угроз).
* Обусловленные техническими средствами (техногенные источники угрозы).
* Обусловленные стихийными источниками.

Антропогенные угрозы – это угрозы которые обусловлены деятельностью человека. К данному типу можно отнести угрозы, возникающие вследствие как непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.п., так и угрозы, возникающие в силу умышленных действий, связанные с корыстными или иными устремлениями людей. К таким угрозам относятся угрозы, связанные с противоречивыми действиями в руководстве и управлении, неадекватными целями, с человеческим фактором.

**Антропогенные угрозы** – это угрозы, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

**Непреднамеренные** (неумышленные, случайные) угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т. п.;

* нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия пользователей ИВС;
* пожары, произошедшие не по причине поджога;
* предоставление несанкционированного доступа к информационным ресурсам компании в результате сбоя ПО;

**Преднамеренные** (умышленные) угрозы, связанные с корыстными, идейными или иными устремлениями людей (злоумышленников).

* деятельность преступных групп и формирований;
* удаленное несанкционированное вмешательство посторонних лиц;
* преднамеренные угрозы целостности оборудования компании со сторон сотрудников компании или лиц и организаций, не входящих в состав компании;
* пожары, произошедшие по причине поджога.

Техногенные угрозы – это угрозы, обусловленные воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека. К такому типу угроз, можно отнести сбои, в том числе в работе, или разрушение систем, созданных человеком.

Естественные (природных) угрозы – это угрозы, обусловленные воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека. К данному типу угроз относятся угрозы метеорологического характера, атмосферные, геофизические, геомагнитные и прочие, включая экстремальные климатические условия, метеорологические явления, стихийные бедствия.

Сам источник таких угроз, может являться, по отношению к инфраструктуре компании, как внешним, так и внутренним.

**Внешние угрозы**

На программное средство(ПС):

* Некорректный исходный алгоритм;
* Неправильно запрограммированный исходный алгоритм;

На аппаратные средства

* Системные ошибки при постановке задачи проектирования;
* Отклонения от технологии изготовления комплектующих изделий и АС в целом;
* Нарушение режима эксплуатации, вызванное внутренним состоянием АС.

**Внутренние угрозы:**

На программное средство(ПС):

* Неквалифицированные пользователи;
* Несанкционированный доступ к ПС с целью модификации кода;

На аппаратные средства

* Внешние климатические условия;
* Электромагнитные и ионизирующие помехи;
* Перебои в электроснабжении;
* Недостаточная квалификация обслуживающего персонала.

1. **Оценка угроз, рисков и уязвимостей**

После идентификации угроз и уязвимостей необходимо оценить вероятность их объединения и возникновения риска. Это включает в себя оценку вероятности реализации угроз, а также того насколько легко они могут использовать имеющиеся уязвимости.

Оценка вероятности угроз должна учитывать природу угроз и особенности, присущие различным группам угроз, например:

Преднамеренные угрозы. Вероятность преднамеренных угроз зависит от мотивации, знаний, компетенции и ресурсов, доступных потенциальному злоумышленнику, а также от привлекательности активов для реализации атак.

Случайные угрозы. Вероятность случайных угроз может оцениваться с использованием статистики и опыт. Вероятность таких угроз может зависеть от близости организации к источникам опасности. Также географическое положение организации оказывает влияние на возможность возникновения экстремальных погодных условий. Вероятность человеческих ошибок и поломки оборудования также должны быть оценены.

Прошлые инциденты. Инциденты, происходившие в прошлом, иллюстрирующие проблемы в существующих защитных мерах.

Новые разработки и тенденции. Они включают в себе отчеты, новости и тенденции, полученные из Интернета, групп новостей, от других организаций и консультантов.

Для оценки значимости угроз, необходимо предварительно составить таблицу условной численной шкалы для оценки финансового ущерба компании.

Таблица 5.1 – Условная численная шкала для оценки ущерба

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 0 | Инцидент принесет ничтожный моральный и финансовый ущерб компании |
| 1 | Ущерб от инцидента есть, но он незначителен, основные финансовые операции и положение компании на рынке не затронуты |
| 2 | Финансовые операции не ведутся в течение некоторого времени, за это время компания терпит убытки, но её положение на рынке и количество клиентов изменяются минимально |
| 3 | Значительные потери на рынке и в прибыли. От компании уходит ощутимая часть клиентов |
| 4 | Потери очень значительны, компания на период до года теряет положение на рынке. Для восстановления положения требуются крупные финансовые займы |

Продолжение таблицы 5.1

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 5 | Компания прекращает существование |

Вероятность того, что угроза реализуется, определяется на основе следующих факторов:

* привлекательность ресурса как показатель при рассмотрении угрозы от умышленного воздействия со стороны человека;
* возможность использования ресурса для получения дохода как показатель при рассмотрении угрозы от умышленного воздействия со стороны человека;
* технические возможности угрозы, используемые при умышленном воздействии со стороны человека;
* вероятность того, что угроза реализуется;
* степень легкости, с которой уязвимость может быть использована.

Также необходимо составить вероятностно-временную шкалу реализации угрозы информационным ресурсам.

Таблица 5.2 - Вероятностно-временная шкала реализации угрозы

|  |  |
| --- | --- |
| Вероятность угрозы | Средняя частота угрозы |
| 0 | Данный вид угрозы отсутствует |
| 0.1 | Реже, чем раз в год |
| 0.2 | Около 1 раза в год |
| 0.3 | Около 1 раза в месяц |
| 0.4 | Около 1 раза в неделю |
| 0.5 | Практически ежедневно |

Как видно из Таблицы 5.2 наиболее опасными являются угрозы вероятность которых составляет 0.3 – 0.5. Соответственно при разработке политики информационной безопасности наибольшее внимание стоит уделить таким угрозам.

1. **Методы, меры и средства обеспечения требуемого уровня защиты информационных ресурсов.**

Методы защиты информации классифицируются:

* Препятствие - создание на пути [угрозы](http://aguryanov.blogspot.com/2012/09/blog-post_6947.html) преграды, преодоление которой сопряжено с возникновением сложностей для злоумышленника или дестабилизирующего фактора.
* Управление - оказание управляющих воздействий на элементы защищаемой системы.
* Маскировка - действия над защищаемой системой или информацией, приводящие к такому их преобразованию, которое делает их недоступными для злоумышленника. (Сюда можно, в частности, отнести [криптографические методы защиты](http://aguryanov.blogspot.com/2012/09/blog-post_3412.html) ).
* Регламентация - разработка и реализация комплекса мероприятий, создающих такие условия обработки информации, которые существенно затрудняют реализацию атак злоумышленника или воздействия других дестабилизирующих факторов.
* Принуждение - метод заключается в создании условий, при которых пользователи и персонал вынуждены соблюдать условия обработки информации под угрозой ответственности (материальной, уголовной, административной)
* Побуждение - метод заключается в создании условий, при которых пользователи и персонал соблюдают условия обработки информации по морально-этическим и психологическим соображениям.

Таблица 6.1 – Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск |
| Наблюдение за источниками информации | 2 | 0.3 | 0.6 |
| Кражи, нападения, взлом, саботаж и проникновение | 3 | 0.1 | 0.5 |
| Подслушивание конфиденциальных разговоров и акустических сигналов работающих механизмов | 3 | 0.3 | 0.9 |

Продолжение таблицы 6.1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск | |
| Разглашение информации компетентными людьми | 3 | 0.3 | 0.9 | |
| Отказы и неисправности технических средств | 1 | 0.2 | 0.2 | |
| Атаки на уровне приложений | 3 | 0.2 | 0.7 | |
| Утеря носителей информации | 3 | 0.1 | 0.3 | |
| Воздействие стихийных сил | 2 | 0.2 | 0.4 | |
| Парольные атаки | 4 | 0.4 | 0.9 | |
| Сбой и отказы в аппаратуре сбора, обработки и передачи информации | 2 | 0.2 | 0.4 | |
| Отказы системы электроснабжения | 2 | 0.3 | 0.6 | |
| Фишинг | 4 | 0.4 | | 1 | |
| Воздействие мощных электромагнитных и электрических помех (промышленных и природных) | 2 | 0.2 | | 0.4 | |
| Переполнение буфера | 2 | 0.2 | | 0.4 | |

Информационную безопасность логистической компании должны обеспечивать комплекс мер, которые классифицируются:

* административные;
* организационные;
* технические.

Все меры для своей эффективности, должны применяться совместно.

Административные меры – включают в себя разработку внутренних нормативных документов, обеспечивающих информирование сотрудников о системе действий, необходимых для обеспечения информационной безопасности. Такие документы хранятся в открытом доступе, и в компании все сотрудники должны с ними ознакомиться.

Организационные меры – в большей степени они направлены на устранение внутренней угрозы утечки информации и мотивацию сотрудников на соблюдение утвержденных регламентов. Эти меры предпринимаются службой безопасности во взаимодействии с сотрудниками служб управления персоналом.

Технические меры - эта группа мер рассчитана на использование действенных технических средств защиты. Для ее реализации используются аппаратные, программные и криптографические средства.

Меры применимы для обеспечения информационной безопасности:

* установление различных степеней допуска сотрудников к сведениям, содержащим коммерческую тайну;
* ограничение круга лиц, имеющих допуск к конфиденциальной информации страховой компании;
* организация порядка использования материальных носителей, установление контроля над копированием и сканированием документов, ограничение доступа сотрудников к внешней электронной почте;
* проведение периодических проверок соблюдения регламентов;
* привлечение специалистов для проведения тренингов по защите информации;
* проведение мероприятий по созданию режима коммерческой тайны;
* внесение в договоры компании с клиентами норм, касающихся обязательств соблюдения последними режима коммерческой тайны в отношении переданной им информации;
* привлечение к ответственности лиц, виновных в разглашении информации.

**Вывод**

Политика безопасности — совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. Основная цель политики безопасности – определение технических требований к защите компьютерных систем и сетевой аппаратуры, способы настройки систем администратором с точки зрения их безопасности.

На сегодняшний день проблема информационной защиты не является новой. Её появление началось ещё до появления компьютеров. Однако появление и стремительный рост компьютерной техники, а также значимость её в жизни сказалось и на основные принципы построения политики информационной защиты.

Существует определённый набор правил, которые желательно придерживаться при организации защиты информации:

* создание и эксплуатация систем защиты информации является сложным и ответственным процессом. Не доверяйте вопросы защиты информации дилетантам, поручите их профессионалам;
* не старайтесь организовать абсолютно надежную защиту - такой просто не существует. Система защиты должна быть достаточной, надежной, эффективной и управляемой. Эффективность защиты информации достигается не количеством денег, потраченных на ее организацию, а способностью ее адекватно реагировать на все попытки несанкционированного доступа к информации;
* мероприятия по защите информации от несанкционированного доступа должны носить комплексный характер, т.е. объединять разнородные меры противодействия угрозам;
* основная угроза информационной безопасности компьютерных систем исходит непосредственно от сотрудников. С учетом этого необходимо максимально ограничивать как круг сотрудников, допускаемых к конфиденциальной информации, так и круг информации, к которой они допускаются. При этом каждый сотрудник должен иметь минимум полномочий по доступу к конфиденциальной информации.

Лучшая защита от нападения — это не допустить его. Обучение пользователей правилам сетевой безопасности может предотвратить нападения. Защита информации включает в себя кроме технических мер еще и обучение или правильный подбор обслуживающего персонала. Защита информации не ограничивается техническими методами. Основной недостаток защиты — люди, и поэтому надежность системы безопасности зависит в основном от отношения к ней. Помимо этого, защита должна постоянно совершенствоваться вместе с развитием компьютерной сети.