Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**«Отчёт по лабораторной работе №1**

“Разработка и внедрение политики безопасности логистической компании”

**Выполнил:** студент 3 курса

4 группы специальности ПОИТ

Примаков Максим Николаевич

**Проверил:** преподаватель

Блинова Евгения Александровна

Минск 2020

**Цель работы:** приобретение практических навыков разработки и внедрения эффективной политики информационной безопасности организации или учреждения.

1. **Актуальность, цели и задачи разработки ПИБ.**

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. Обеспечение ИБ в этой сфере и, в частности, основные требования, организационные правила и процедуры непосредственно регламентируются указанными в начале данного подраздела документами.

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.

1. **Объекты защиты.**

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

Структура логитсической компании



Рисунок 1

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 несут 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 уходам денежных средств, и отвечает за начисление з\п 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. 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.**

Все угрозы информационной безопасности делятся на три типа по природе их возникновения: антропогенные, техногенные и естественные.

* 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.
* 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.

К естественным относятся природные явления, которые не зависят от человека, например ураганы, наводнения, пожары и т.д.

**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.;

1. нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия пользователей ИВС

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

1. деятельность преступных групп и формирований;
2. удаленное несанкционированное вмешательство посторонних лиц;

* **Внешние угрозы**

1. На программное средство(ПС):

* Некорректный исходный алгоритм;
* Неправильно запрограммированный исходный алгоритм;

1. 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:**

1.На программное средство(ПС):

* неквалифицированные пользователи;
* несанкционированный доступ к ПС с целью модификации кода;

2. На аппаратные средства

* внешние климатические условия;
* электромагнитные и ионизирующие помехи;
* перебои в электроснабжении;
* недостаточная квалификация обслуживающего персонала.

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

**Угрозы**

1) кражи, удаления или модификации информации, несанкционированного распространение материальных носителей за пределами организации);

2) наблюдение за клиентами компании;

3) подслушивание конфиденциальных разговоров;

4) перехват электрических, магнитных и электромагнитных полей, электрических сигналов и радиоактивных излучений;

5) разглашение информации о пользователях;

6) утеря носителей информации;

7) воздействие стихийных сил (наводнения, пожары и т. п.);

8) сбои и отказы в аппаратуре сбора, обработки и передачи информации;

9) отказы системы электроснабжения;

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

* 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.

Таблица 1

**Оценка рисков**

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск  (Ущерб  \*Вероятность) |
| наблюдение за источниками информации | 2 | 0.3 | 0.6 |
| подслушивание конфиденциальных разговоров и акустических сигналов работающих механизмов | 3 | 0.3 | 0.9 |
| разглашение информации компетентными людьми | 3 | 0.3 | 0.9 |
| утеря носителей информации | 3 | 0.1 | 0.3 |
| воздействие стихийных сил | 2 | 0.2 | 0.4 |
| сбои и отказы в аппаратуре сбора, обработки и передачи информации | 2 | 0.2 | 0.4 |
| отказы системы электроснабжения | 2 | 0.3 | 0.6 |
| воздействие мощных электромагнитных и электрических помех (промышленных и природных) | 2 | 0.2 | 0.4 |

**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.

Оглавление

[**1.** **Актуальность, цели и задачи разработки ПИБ.** 2](#_Toc51664196)

[**2.** **Объекты защиты.** 2](#_Toc51664197)

[3. **Основные угрозы.** 3](#_Toc51664198)

[**4.** **Оценка угроз, рисков и уязвимостей.** 4](#_Toc51664199)

[**5.** **Методы, меры и средства обеспечения требуемого уровня защиты информационных ресурсов.** 4](#_Toc51664200)

[**Вывод:** 5](#_Toc51664201)