

1. Описание предприятия

Автосервис «Аста-Авто».

Пользователей – 6.

Компьютеров – 7.

Режим многопользовательский.

Есть выход в интернет.

Система распределенная.

Обрабатываемых данных больше 500 и меньше 5000.

Нужно защитить персональные данные.

Автосервис включает в себя следующие отделы:

1. Малярный цех;
2. Основной цех;
3. отдел приема клиентов.

Уровни конфиденциальности:

1. персональные данные;
2. информация для служебного пользования.

В автосервисе имеются следующие должности:

1. Генеральный директор;
2. Главный бухгалтер;
3. менеджер по продажам (2);
4. Менеджер по работе с клиентами
5. Слесарь

Характеристика информационной системы предприятия

Автосервис использует следующее программное обеспечение:

- пакет Microsoft Office;
- 1С Предприятие 8.
- скидка 0.1 (программа для расчета и учета накопительных скидок);
- Контур
- Банк-клиент

Персональный компьютер есть только у директора (анализирует работу предприятия, планирования деятельности и т.п.), у главного бухгалтера (рассчитывает заработную плату, ведет учет ведения склада, расчеты с поставщиками, и учет денежных расходов автосервиса) и у кассира (проводит денежные операции). Кассиров всего три.

Другие компьютеры персональными не являются и их используют другие работники в своих целях, входя в систему под своим логином и паролем.

Для безопасного доступа пользователей локальной сети в Интернет, для защиты компьютеров от вторжений хакеров, вирусов, спама, точного подсчета трафика используется Интернет-шлюз Advanced на платформе Windows. В состав программного обеспечения входят прокси-сервер, межсетевой экран, антивирусная защита, система обнаружения атак, система анализа содержимого трафика, анти-спам.

Так как предприятие хранит персональные данные покупателя, не подлежащие разглашению (т.е. доступ к которым разрешен не всем), в автосервисе установлена система считывания индивидуальных электронных карт. Эти карты позволяют покупателю получить товары со скидкой. Персональные данные видит только кассир во время считывания карты. Такая система позволяет избежать использования личной информации и настроек данного клиента другим пользователем.

Так же для защиты помещений от несанкционированного доступа, в залах установлены камеры видеонаблюдения, система сигнализации, система противопожарной безопасности, радиочастотная противокражная система.

Актуальность проблемы защиты информации в автосервисе

Обеспечение защиты информации в автосервисе предусматривает необходимость защиты персональных данных. Наиболее важной представляется защита персональных данных, так как доверие клиентов в первую очередь основывается на предоставлении своих личных данных, и соответственно, сохранением их сотрудниками организации.

Поэтому целью обеспечения безопасности в автосервисе является разработка политики безопасности и обеспечение надежной защиты информации на предприятии для его нормального функционирования.

Задачи

В данном индивидуальном задании практиканта поставлены следующие задачи:

1. определить цели и задачи защиты информации в автосервисе;
2. составить матрицу доступа;
3. определить группу требований к автоматизированной системе (далее будет использовано сокращение АС);
4. определить предмет защиты на предприятии;
5. выявить возможные угрозы защищаемой информации в автосервисе и их структуру;
6. выявить источники, виды и способы дестабилизирующего воздействия на защищаемую информацию на предприятии;
7. выявить каналы и методы несанкционированного доступа к защищаемой информации на предприятии;
8. определить основные направления, методы и средства защиты информации на предприятии.

2. Цели и задачи защиты информации в автосервисе

Целями защиты информации предприятия являются:

- предупреждение хищения, утечки, утраты, искажения, подделки конфиденциальной информации (персональных данных);
- предотвращение угроз безопасности личности и предприятия;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию конфиденциальной информации;
- предотвращение других форм незаконного вмешательства в информационные ресурсы и системы, обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющих в информационных системах;
- сохранение, конфиденциальности документированной информации в соответствии с законодательством.

К задачам защиты информации на предприятии относятся:

- обеспечение управленческой, финансовой и маркетинговой деятельности предприятия режимным информационным обслуживанием, то есть снабжением всех служб, подразделений и должностных лиц необходимой информацией, как засекреченной, так и несекретной. При этом деятельность по защите информации по возможности не должна создавать больших помех и неудобств в решении производственных и прочих задач, и в то же время способствовать их эффективному решению, давать предприятию преимущества перед конкурентами и оправдывать затраты средств на защиту информации.
- гарантия безопасности информации, ее средств, предотвращение утечки защищаемой информации и предупреждение любого несанкционированного доступа к носителям засекреченной информации;
- отработка механизмов оперативного реагирования на угрозы, использование юридических, экономических, организационных, социально-психологических, инженерно-технических средств и методов выявления и нейтрализации источников угроз безопасности предприятия;
- документирование процесса защиты информации, особенно сведений с тем, чтобы в случае возникновения необходимости обращения в правоохранительные органы, иметь соответствующие доказательства, что предприятие принимало необходимые меры к защите этих сведений;
- организация специального делопроизводства, исключающего несанкционированное получение конфиденциальной информации.

3. Матрица доступа

Основой политики безопасности является избирательное управление доступом, которое подразумевает, что все субъекты и объекты системы должны быть идентифицированы; права доступа субъекта к объекту системы определяются на основании некоторого правила (свойство избирательности).

Для описания свойств избирательного управления доступом применяется модель системы на основе матрицы доступа (МД), иногда ее называют матрицей контроля доступа. Матрица доступа представляет собой прямоугольную матрицу, в которой объекту системы соответствует строка, а субъекту столбец. На пересечении столбца и строки матрицы указывается тип разрешенного доступа субъекта к объекту. Обычно выделяют такие типы доступа субъекта к объекту, как «доступ на чтение», «доступ на запись», «доступ на исполнение» и др.

Множество объектов и типов доступа к ним субъекта может изменяться в соответствии с некоторыми правилами, существующими в данной системе. Определение и изменение этих правил также является задачей МД.

Начальное состояние системы определяется матрицей доступа, все действия регламентированы и зафиксированы в данной матрице.

R – чтение из объекта;

W – запись в объект;
 CR – создание объекта;
 D – удаление объекта;
 “+” – определяет права доступа для данного субъекта;
 “-” – не определяет права доступа для данного субъекта.

Состояние системы считается безопасным, если в соответствии с политикой безопасности субъектам разрешены только определённые типы доступа к объектам (в том числе отсутствие доступа).

Объектами защиты на предприятии являются:

O1 – технические средства приема, передачи и обработки информации;
 O2 – персональные данные покупателей;
 O3 – персональные данные работников;
 O4 – документированная информация;
 O5 – личные дела работников;
 O6 – электронные базы данных работников и покупателей;
 O7 – средства защиты информации (антивирусные программы, система сигнализации, система противопожарной охраны и др.);

Субъектами доступа к ресурсам предприятия являются:

S1 – генеральный директор;
 S2 – главный бухгалтер;
 S4 – менеджер по продажам;
 S4 – менеджер по работе с клиентами;

Таблица 1. Матрица доступа

	O1	O2	O3	O4	O5	O6	O7	S2	S3	S4
S1	R	R	R,W	R,W	R,W	R,W	R	+	+	+
S2	R,W	-	R	R,W	R	-	-	-	-	-
S3	R,W , DC R	R,W, DCR	R,W, DCR	R,W, DCR	R,W, DCR	R,W, DCR	R,W, R,W	-	+	-
S4	R	R	R	R,W	-	R,W, DCR	R,W, DCR	-	-	-

4. Требования по защите информации от НСД

Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа.

В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД, условно состоящей из следующих четырех подсистем:

- управления доступом;
- регистрации и учета;
- криптографической;
- обеспечения целостности.

Формализованные требования к защите компьютерной информации АС.

Существует 3 группы АС с включающими в себя требованиями по защите систем. Но, учитывая структуру автосервиса, рассматривается первая группа АС (в соответствии с используемой в классификацией), как включающую в себя наиболее распространенные многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности. Причем не все пользователи имеют право доступа ко всей информации АС.

5. Объекты и предметы защиты в автосервисе

Основными объектами защиты в автосервисе являются:

1. персонал (так как эти лица допущены к работе с охраняемой законом информацией (персональные данные) либо имеют доступ в помещения, где эта информация обрабатывается);
2. объекты информатизации – средства и системы информатизации, технические средства приема, передачи и обработки информации, помещения, в которых они установлены, а также помещения, предназначенные для проведения служебных совещаний;
3. информация ограниченного доступа, а именно:
 - персональные данные работников (фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное положение, образование, профессия, уровень квалификации, доход, наличие судимостей и некоторая другая информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника);
 - персональные данные покупателей (фамилия, имя, отчество, дата рождения, телефон, данные о персональных картах и привилегиях покупателя);
4. защищаемая от утраты общедоступная информация:
 - документированная информация, регламентирующая статус предприятия, права, обязанности и ответственность его работников (устав, журнал регистрации, учредительный договор, положение о деятельности, положения о структурных подразделениях, должностные инструкции работников);
 - информация, которая может служить доказательным источником в случае возникновения конфликтных ситуаций (расписки);
5. материальные носители охраняемой законом информации (личные дела работников, личные дела покупателей, электронные базы данных работников и покупателей, бумажные носители и электронные варианты приказов, постановлений, планов, договоров, отчетов);
6. средства защиты информации (антивирусные программы, архиватор данных, программа для создания и восстановления резервной копии Windows, шифрование);
7. технологические отходы (мусор), образовавшиеся в результате обработки охраняемой законом информации (данные о бывших покупателях и сотрудниках).

Предметом защиты информации в автосервисе являются носители информации, на которых зафиксированы, отображены защищаемые сведения:

- база данных о покупателях и сотрудниках предприятия в бумажном и электронном виде;
- приказы, постановления, положения, инструкции, соглашения и обязательства о неразглашении, распоряжения, договоры, планы, отчеты, ведомость ознакомления с Положением о конфиденциальной информации и другие документы в бумажном и электронном виде.

6. Угрозы защищаемой информации в автосервисе

Внешние угрозы:

- конкуренты;
- несанкционированный доступ к информации (хакеры, взломщики)
- вирусы;
- чрезвычайные ситуации;
- шпионские программы (флешки и т.п.);
- несанкционированное копирование;
- кража программно-аппаратных средств.

Внутренние угрозы:

- разглашение конфиденциальной информации сотрудниками предприятия;
- нарушение целостности данных со стороны персонала предприятия;
- потеря информации на жестких носителях;
- угрозы целостности баз данных;
- угрозы целостности программных механизмов работы предприятия;

- делегирование лишних или неиспользуемых полномочий на носитель с конфиденциальной информацией, открытие портов;
- системные сбои;
- повреждение аппаратуры, отказ программного или аппаратного обеспечения;
- угрозы технического характера;
- угрозы нетехнического или некомпьютерного характера – отсутствие паролей, конфиденциальная информация, связанная с информационными системами хранится на бумажных носителях.

7. Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию

К источникам дестабилизирующего воздействия относятся:

- люди;
- технические средства отображения (фиксации), хранения, обработки, воспроизведения, передачи информации, средства связи и системы обеспечения их функционирования;
- природные явления.

Виды и способы дестабилизирующего воздействия на защищаемую информацию дифференцируются по источникам воздействия. Самое большее количество видов и способов дестабилизирующего воздействия имеет отношение к людям.

Со стороны людей возможны следующие виды воздействия, приводящие к уничтожению, искажению и блокированию:

- непосредственное воздействие на носители защищаемой информации;
- несанкционированное распространение конфиденциальной информации;
- вывод из строя технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи;
- нарушение режима работы перечисленных средств и технологии обработки информации;
- вывод из строя и нарушение режима работы систем обеспечения функционирования названных средств.

Несанкционированное распространение конфиденциальной информации может осуществляться путем:

- словесной передачи (сообщения) информации;
- передачи копий (снимков) носителей информации;
- показа носителей информации;
- ввода информации в вычислительные сети;
- опубликования информации в открытой печати;
- использования информации в открытых публичных выступлениях, в т.ч. по радио, телевидению;
- потеря носителей информации.

Способами нарушения режима работы технических средств отображения, хранения, обработки, воспроизведения, передача информации, средств связи и технологии обработки информации, приводящими к уничтожению, искажению и блокированию информации, могут быть:

- повреждение отдельных элементов средств;
- нарушение правил эксплуатации средств;
- внесение изменений в порядок обработки информации;
- заражение программ обработки информации вредоносными программами;
- выдача неправильных программных команд;
- превышение расчетного числа запросов;
- передача ложных сигналов – подключение подавляющих фильтров в информационные цепи, цепи питания и заземления;
- нарушение (изменение) режима работы систем обеспечения функционирования средств.

К видам дестабилизирующего воздействия на защищаемую информацию со стороны технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи и систем обеспечения их функционирования относятся:

- выход средств из строя;
- сбои в работе средств
- создание электромагнитных излучений.

8. Каналы и методы несанкционированного доступа к защищаемой информации в автосервисе

К числу наиболее вероятных каналов утечки информации можно отнести:

- визуальное наблюдение;
- подслушивание;
- техническое наблюдение;
- прямой опрос, выведывание;
- ознакомление с материалами, документами;
- сбор открытых документов и других источников информации;
- хищение документов и других источников информации;
- изучение множества источников информации, содержащих по частям необходимые сведения.

9. Организация комплексной системы защиты информации в автосервисе

Для организации эффективной защиты конфиденциальной информации необходимо разработать программу, которая должна позволить достигать следующие цели:

- обеспечить обращение сведений в заданной сфере;
- предотвратить кражу и утечку конфиденциальной информации, любую порчу конфиденциальной информации;
- документировать процесс защиты данных, чтобы в случае попыток незаконного завладения какими-либо данными предприятия можно было защитить свои права юридически и наказать нарушителя.

Программа будет отражать размер данного предприятия, тип технологии и деловой информации, которую необходимо защищать.

В программе должны учитываться возможные источники и каналы утечки информации.

Для построения системы защиты конфиденциальной информации на предприятии необходимо создание службы защиты информации (далее – СлЗИ), которая будет являться структурной единицей предприятия, непосредственно участвующей в производственно-коммерческой деятельности. Работа этого отдела проводится во взаимодействии со структурными подразделениями предприятия. Структура и штат СлЗИ в зависимости от объема работ и особенностей производственно-коммерческой деятельности определяются руководителем предприятия и, как правило, должны комплектоваться инженерно-техническими работниками – специалистами основного профиля работы данного предприятия, а также специалистами, имеющими практический опыт защиты информации или работы с различными группами людей. Назначение на должность начальника СлЗИ предприятия, а также его освобождение производится только руководителем предприятия. Руководитель службы защиты информации регулярно, в установленные сроки отчитывается в своей работе перед директором предприятия.

Система доступа к конфиденциальным данным, должна обеспечить безусловное ознакомление с такими материалами только тех лиц, которым они нужны по службе. Система доступа к конфиденциальной информации – есть комплекс административно-правовых норм, обеспечивающих получение необходимой для работы информации каждым исполнителем и руководителем секретных работ. Цель системы – обеспечить только санкционированное получение необходимого объема конфиденциальной информации. В структуру этой системы входят:

- разрешительная система доступа к документальной конфиденциальной информации;

– система пропусков и шифров, обеспечивающая только санкционированный доступ в помещения, где ведутся секретные работы.

Для обеспечения физической сохранности носителей засекреченной информации и предотвращения доступа посторонних лиц нужна система охраны, которая включает в себя комплекс мероприятий, сил и средств, задействованных для предотвращения доступа посторонних лиц к носителям защищаемой информации.

Заключение

В процессе выполнения индивидуального задания практикантам была поставлена задача – создать и проанализировать средства информационной безопасности автосервиса «Аста-Авто». Поставленные цели были достигнуты при помощи классифицирования предприятия, были предложены методы и средства для усовершенствования политики безопасности данного предприятия, в результате выполнения которых предприятие позволит повысить эффективность средств защиты и сократит риск потери и искажения информации.

Следует обратить внимание на то, что только при совместном взаимодействии персонала, программно-аппаратных средств и средств защиты информации возможна эффективность данных мероприятий.

Данное предприятие циркулирует большим количеством информации конфиденциального характера, доступ к которой необходимо ограничить. Поэтому, целью являлась разработка такой системы по защите информации, при которой угрозы утечки конфиденциальной информации были бы минимальны.

В результате анализа была построена модель информационной системы с позиции безопасности.

Никакие аппаратные, программные и любые другие решения не смогут гарантировать абсолютную надежность и безопасность данных в компьютерных сетях. В то же время свести риск потерь к минимуму возможно лишь при комплексном подходе к вопросам безопасности.