После построения модели необходимо оценить ее качество. Для этого используется коэффициент детерминации, который равен 0,998, что говорит о хороших показателях качества модели.

В качестве примера использования полученной модели была проведена оценка квартиры, находящейся по адресу ул. Ферганская, дом 65а, со следующими характеристиками:

1. стоимость объекта недвижимости – 1430 тыс. руб.;
2. количество комнат – 1;
3. общая площадь жилья – 24 кв. м.;
4. площадь кухни – 5 кв. м.;
5. отделка – евроремонт;
6. тип постройки – кирпичный;
7. средняя стоимость кв. м в зависимости от района – ленинский;
8. жилая площадь – 15 кв. м;
9. санузел – совмещенный;
10. этаж – первый.

По указанным характеристикам рассчитываются значения регрессионных переменных x1, x2, x3, x4, x5, x6, x7, x8, x9 и подставляются в уравнение и получаем значение 1556,52 тыс. руб.

Заключение

В ходе выполнения работы были собраны и обработаны данные объявлений о продаже квартир с разных интернет-ресурсов. Первоначально в выборку входило 12 переменных, но после использования метода главных компонент и проверки на мультиколлинеарность, осталось девять переменных. Выборка была проверена на гетероскедастичность, с последующим устранением выше сказанного явления.

Была построена модель и проверена на адекватность найденных параметров. А так же использование полученной модели на реальном объекте.

Предполагается дальнейшее использование полученной регрессии при создании автоматизированной системы расчета стоимости недвижимости на основе сравнительного подхода.

Литература.

1. Pingola – недвижимость. URL: http://tomsk.pingola.ru/realty/sale/kvartira.
2. Единое информационное пространство недвижимости. Обзор томского рынка квартир. [Электронный ресурс]. – Режим доступа: http://www.eip.ru/main/view4965 свободный.
3. Региональный фонд капитального ремонта многоквартирных домов Томской области. [Электронный ресурс]. – Режим доступа: http://kaprem.tomsk.ru/reg_programm/?ELEMENT_ID=211 свободный.
4. Айвазян С.А., Мхитарян В.С. Прикладная статистика и основы эконометрики: Учебник для вузов. М.: ЮНИТИ, 1998. – 1005с

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

А.К. Курманбай, студент группы 17В41,
научный руководитель: Разумников С.В.ассистент
Юргинский технологический институт (филиал) Национального исследовательского Томского политехнического университета
652055, Кемеровская обл., г. Юрга, ул. Ленинградская, 26, тел: +79059675373,
E-mail: aigera_0796@mail.ru

Вопрос безопасности и защита информации от несанкционированного доступа стоит сегодня на первом месте по степени насущности. Случаи хищения интеллектуальной собственности, промышленного шпионажа, получение несанкционированного доступа к персональным данным и стратегически важным информационным ресурсам организаций случаются все чаще и носят все более серьезный и угрожающий характер. Масштабы могут быть самыми разными, но суть одна.

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).

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.

Средства защиты информации:

Физические средства механические, электрические, электромеханические, электронные, электронно-механические и т. п. устройства и системы, которые функционируют автономно, создавая различного рода препятствия на пути дестабилизирующих факторов.

Аппаратные средства различные электронные и электронно-механические и т.п. устройства, схемно встраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач защиты информации.

Программные средства специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения с целью решения задач защиты информации.

Организационные средства организационно-технические мероприятия, специально предусматриваемые в технологии функционирования системы с целью решения задач защиты информации.

Законодательные средства нормативно-правовые акты, с помощью которых регламентируются права и обязанности, а также устанавливается ответственность всех лиц и подразделений, имеющих отношение к функционированию системы, за нарушение правил обработки информации, следствием чего может быть нарушение ее защищенности.

Психологические (морально-этические средства) сложившиеся в обществе или данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение их приравнивается к несоблюдению правил поведения в обществе или коллективе.

Методы обеспечения безопасности информации в ИС: препятствие; управление доступом; механизмы шифрования; противодействие атакам вредоносных программ; регламентация; принуждение; побуждение.

Препятствие – метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.д.). Управление доступом – методы защиты информации регулированием использования всех ресурсов ИС и ИТ. Эти методы должны противостоять всем возможным путям несанкционированного доступа к информации.

Управление доступом включает следующие функции зашиты: идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора); опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору; проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту); разрешение и создание условий работы в пределах установленного регламента; регистрацию (протоколирование) обращений к защищаемым ресурсам; реагирование (сигнализация, отключение, задержка работ, отказ в запросе и т.п.) при попытках несанкционированных действий.

Механизмы шифрования – криптографическое закрытие информации. Эти методы защиты все шире применяются как при обработке, так и при хранении информации на магнитных носителях. При передаче информации по каналам связи большой протяженности этот метод является единственно надежным.

Противодействие атакам вредоносных программ предполагает комплекс разнообразных мер организационного характера и использование антивирусных программ. Цели принимаемых мер – это уменьшение вероятности инфицирования АИС, выявление фактов заражения системы; уменьшение последствий информационных инфекций, локализация или уничтожение вирусов; восстановление информации в ИС. Овладение этим комплексом мер и средств требует знакомства со специальной литературой.

Регламентация – создание таких условий автоматизированной обработки, хранения и передачи защищаемой информации, при которых нормы и стандарты по защите выполняются в наибольшей степени.

Принуждение – метод защиты, при котором пользователи и персонал ИС вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Побуждение – метод защиты, побуждающий пользователей и персонал ИС не нарушать установленные порядки за счет соблюдения сложившихся моральных и этических норм.

Вся совокупность технических средств подразделяется на аппаратные и физические.

Аппаратные средства – устройства, встраиваемые непосредственно в вычислительную технику, или устройства, которые сопрягаются с ней по стандартному интерфейсу.

Физические средства включают различные инженерные устройства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты и осуществляющие защиту персонала (личные средства безопасности), материальных средств и финансов, информации от противоправных действий. Примеры физических средств: замки на дверях, решетки на окнах, средства электронной охранной сигнализации и т.п.

Программные средства – это специальные программы и программные комплексы, предназначенные для защиты информации в ИС. Как отмечалось, многие из них слиты с ПО самой ИС.

Из средств ПО системы защиты выделим еще программные средства, реализующие механизмы шифрования (криптографии). Криптография – это наука об обеспечении секретности и/или аутентичности (подлинности) передаваемых сообщений.

Организационные средства осуществляют своим комплексом регламентацию производственной деятельности в ИС и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становится невозможным или существенно затрудняется за счет проведения организационных мероприятий. Комплекс этих мер реализуется группой информационной безопасности, но должен находиться под контролем первого руководителя.

В настоящее время в США разработан стандарт оценок безопасности компьютерных систем – критерии оценок пригодности. В нем учитываются четыре типа требований к компьютерным системам:

- требования к проведению политики безопасности – security policy;
- ведение учета использования компьютерных систем – accounts;
- доверие к компьютерным системам;
- требования к документации.

Только после оценки безопасности компьютерной системы она может поступить на рынок.

Во время эксплуатации ИС наибольший вред и убытки приносят вирусы. Защиту от вирусов можно организовать так же, как и защиту от несанкционированного доступа. Технология защиты является многоуровневой и содержит следующие этапы:

1. Входной контроль нового программного обеспечения или дискеты, который осуществляется группой специально подобранных детекторов, ревизоров и фильтров. Например, в состав группы можно включить Scan, Aidstest, TPU8CLS. Можно провести карантинный режим. Для этого создается ускоренный компьютерный календарь. При каждом следующем эксперименте вводится новая дата и наблюдается отклонение в старом программном обеспечении. Если отклонения нет, то вирус не обнаружен.

2. Сегментация жесткого диска. При этом отдельным разделам диска присваивается атрибут Read Only. Для сегментации можно использовать, например, программу Manager и др.

3. Систематическое использование резидентных, программ-ревизоров и фильтров для контроля целостности информации, например Check21, SBM, Antivirus2 и т.д.

4. Архивирование. Ему подлежат и системные, и прикладные программы. Если один компьютер используется несколькими пользователями, то желательно ежедневное архивирование. Для архивирования можно использовать PKZIP и др.

Эффективность программных средств защиты зависит от правильности действий пользователя, которые могут быть выполнены ошибочно или со злым умыслом.

В связи с этим главное при определении мер и принципов защиты информации это квалифицированно определить границы разумной безопасности и затрат на средства защиты с одной стороны и поддержания системы в работоспособном состоянии и приемлемого риска с другой.

Литература.

1. Мельников В. Защита информации в компьютерных системах. М.: Финансы и статистика, Электронинформ, 1997 – 368 с.
2. ХоффманД.Д. Современные методы защиты информации.- М.: Бином 1980.-330с
3. Ведеев Д. Защита данных в компьютерных сетях. Открытые системы.- М.: Дрофа 1995, №3.-180с
4. Левин В.К. Защита информации в информационно-вычислительных системах и сетях // Программирование.- СПБ.: Питер 1994. - N5.-160 с.