Содержание:

Введение

Понятие информационная безопасность столь обширно, что в него можно вместить практически всё, что связано с защитой информации любого типа.

Это может быть — безопасность информации на уровне государства, а может быть защита личных данных пользователя компьютера. И каждое из этих действий является одинаково важным. В сумме — это действия по защите конфиденциальности, доступности, а также целостности информации. И защищать ее нужно самыми лучшими способами. В наше время кто владеет информацией — владеет миром.

Это могут быть такие простые вещи как защита собственного компьютера от вирусов и взлома, а могут быть более сложные, например соблюдение конфиденциальности информации на предприятии или в фирме.

Последствия пренебрежения средствами защиты информации могут быть серьёзными: украденные личные данные, которые можно использовать в корыстных целях (кража, мошенничество), украденные банковские данные (банковской карты), украденные различные разработки, идеи и материалы.

И все это может навредить Вам лично или организации и компании. А размеры этих последствий будут выражаться не только денежными потерями. Пострадают также репутация и доверие.

Но не смотря на столь пессимистичные прогнозы, выход есть, и он заключается в изучении источников угроз и комплексном применении технологий защиты информации. Кроме того, защита информации должна быть непрерывным процессом, ведь средства атаки на неё так же постоянно прогрессируют.

Глава 1. Основные положения информационной безопасности

1.1. Понятие информационной безопасности

Информация — результат и отражение в человеческом сознании, многообразие внутреннего и окружающего миров (сведения об окружающих человека предметах, явлений, действия других людей).

Информационная безопасность может рассматриваться в следующих значениях:

Состояние (качество) определённого объекта (в качестве объекта может выступать информация, данные, ресурсы автоматизированной системы, автоматизированная система, информационная система предприятия, общества, государства, организации и т. п.);

Деятельность, направленная на обеспечение защищённого состояния объекта (в этом значении чаще используется термин «защита информации»).

Информационная безопасность — это процесс обеспечения конфиденциальности, целостности и доступности информации.

Информационная безопасность — все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, безотказности, подотчётности, аутентичности и достоверности информации или средств её обработки.

Безопасность информации (данных) — состояние защищённости информации (данных), при котором обеспечиваются её (их) конфиденциальность, доступность и целостность.

Безопасность информации (данных) определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые в автоматизированной системе.

Безопасность информации (при применении информационных технологий) — состояние защищённости информации (данных), обеспечивающее безопасность информации, для обработки которой она применяется, и информационную безопасность автоматизированной информационной системы, в которой она реализована.

Безопасность автоматизированной информационной системы — состояние защищённости автоматизированной системы, при котором обеспечиваются конфиденциальность, доступность, целостность, подотчётность и подлинность её

ресурсов.

Информационная безопасность — защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений. Поддерживающая инфраструктура — системы электроснабжения, теплоснабжения, водоснабжения, газоснабжения, системы кондиционирования и т. д., а также обслуживающий персонал. Неприемлемый ущерб — ущерб, которым нельзя пренебречь.

Шушков Г.М., Сергеев И.В. определяют "информационную безопасность" как "процесс баланса между возникающими, воздействующими угрозами и успешностью противодействия этим угрозам со стороны органов государственной власти, отвечающих за безопасность государства".

Ценность информации — является важнейшим критерием при принятии решений о защите информации.

Уровень секретности — административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю секретной конкурентной информации, регламентируемой специальным документом с учетом государственно-стратегических и военно-стратегических, коммерческих, служебных или частных интересов.

Статистика защиты информации показывает, что защищать нужно не только секретную информацию, но и связанную с ней не секретную.

1.2. Принципы информационной безопасности

Под безопасностью автоматизированной информационной системы организации (учреждения) понимается ее защищенность от случайного или преднамеренного вмешательства в нормальный процесс функционирования, а также от попыток хищения, модификации или разрушения ее компонентов. Безопасность системы достигается обеспечением конфиденциальности обрабатываемой ею информации, а также целостности и доступности компонентов и ресурсов системы.

- Конфиденциальность компьютерной информации — это свойство информации быть известной только допущенным и прошедшим проверку (авторизацию) субъектам системы (пользователям, программам, процессам и т. д.).

- Целостность компонента (ресурса) системы — свойство компонента (ресурса) быть неизменным (в семантическом смысле) при функционировании системы.
- Доступность компонента (ресурса) системы — свойство компонента (ресурса) быть доступным для использования авторизованными субъектами системы в любое время.
- Законность/Этичность использования компонента (ресурса) системы — свойство компонента (ресурса) быть соответствующим законодательным и этическим нормам для использования субъектами системы.

Безопасность системы обеспечивается комплексом технологических и административных мер, применяемых в отношении аппаратных средств, программ, данных и служб с целью обеспечения доступности, целостности и конфиденциальности связанных с компьютерами ресурсов; сюда же относятся и процедуры проверки выполнения системой определенных функций в строгом соответствии с их запланированным порядком работы.

Систему обеспечения безопасности системы можно разбить на следующие подсистемы:

- компьютерную безопасность;
- безопасность данных;
- безопасное программное обеспечение;
- безопасность коммуникаций.

Компьютерная безопасность обеспечивается комплексом технологических и административных мер, применяемых в отношении аппаратных средств компьютера с целью обеспечения доступности, целостности и конфиденциальности связанных с ним ресурсов.

Безопасность данных достигается защитой данных от неавторизованных, случайных, умышленных или возникших по халатности модификаций, разрушений или разглашения.

Безопасное программное обеспечение представляет собой общецелевые и прикладные программы и средства, осуществляющие безопасную обработку данных в системе и безопасно использующие ресурсы системы.

Безопасность коммуникаций обеспечивается посредством аутентификации телекоммуникаций за счет принятия мер по предотвращению предоставления неавторизованным лицам критичной информации, которая может быть выдана

системой в ответ на телекоммуникационный запрос.

1.3. Потенциальные угрозы информационной безопасности

Угрозы конфиденциальности данных и программ. Реализуются при несанкционированном доступе к данным (например, к сведениям о состоянии счетов клиентов банка), программам или каналам связи.

Угрозы целостности данных, программ, аппаратуры. Целостность данных и программ нарушается при несанкционированном уничтожении, добавлении лишних элементов и модификации записей, изменении порядка расположения данных, формировании фальсифицированных документов в ответ на законные запросы, при активной ретрансляции сообщений с их задержкой.

Угрозы доступности данных. Возникают в том случае, когда объект (пользователь или процесс) не получает доступа к законно выделенным ему службам или ресурсам. Эта угроза реализуется захватом всех ресурсов, блокированием линий связи несанкционированным объектом в результате передачи по ним своей информации или исключением необходимой системной информации.

Способы воздействия угроз на объекты информационной безопасности подразделяются на информационные, программно-математические, физические, радиоэлектронные и организационно-правовые.

К информационным способам относятся:

- нарушение адресности и своевременности информационного обмена, противозаконный сбор и использование информации;
- несанкционированный доступ к информационным ресурсам;
- манипулирование информацией (дезинформация, сокрытие или искажение информации);
- незаконное копирование данных в информационных системах;
- нарушение технологии обработки информации.

Программно-математические способы включают:

- внедрение компьютерных вирусов;
- установку программных и аппаратных закладных устройств;
- уничтожение или модификацию данных в автоматизированных информационных системах.

Физические способы включают:

- уничтожение или разрушение средств обработки информации и связи;
- уничтожение, разрушение или хищение машинных или других оригинальных носителей информации;
- хищение программных или аппаратных ключей и средств криптографической защиты информации;
- воздействие на персонал;
- поставку «зараженных» компонентов автоматизированных информационных систем.

Радиоэлектронными способами являются:

- перехват информации в технических каналах ее возможной утечки;
- внедрение электронных устройств перехвата информации в технические средства и помещения;
- перехват, дешифровка и навязывание ложной информации в сетях передачи данных и линиях связи;
- воздействие на системы аутентификации;
- радиоэлектронное подавление линий связи и систем управления.

Организационно-правовые способы включают:

- невыполнение требований законодательства и задержки в принятии необходимых нормативно-правовых положений в информационной сфере;
- неправомерное ограничение доступа к документам, содержащим важную для граждан и организаций информацию.

Негативные факторы способствующие реализации угроз информационной безопасности

- Объективные социально-психологические особенности персонала и пользователей
- Нелояльность персонала и пользователей
- Нелояльность посторонних лиц и организаций
- Особенности используемого программного обеспечения
- Вредоносные программы
- Конструктивные и технологические особенности аппаратуры
- Эксплуатационный износ, физическое старение магнитных носителей, возможные отказы оборудования

- Совместная обработка информации разной категории конфиденциальности
- Возможные проблемы с электропитанием
- Неблагоприятные факторы воздействия внешней среды на аппаратуру
- Пожароопасность, возможность стихийных бедствий, аварий и других воздействий техногенного характера
- Технические каналы утечки информации
- Технологический мусор

1.4. Компьютерные преступления

Под компьютерным преступлением следует понимать предусмотренные законом общественно-опасные деяния, совершаемые с использованием средств компьютерной техники. Правомерно также использовать термин «компьютерное преступление» в широком значении как социологическую категорию, а не как понятие уголовного права.

Виды компьютерных преступлений:

- несанкционированный доступ в корыстных целях к информации, хранящейся в компьютере или информационно-вычислительной сети. Несанкционированный доступ осуществляется, как правило, с использованием чужого-имени, изменением физических адресов технических устройств, использованием информации, оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных. Бывает, что некто проникает в компьютерную систему, выдавая себя за законного пользователя. Самый простой путь его осуществления — получить коды и другие идентифицирующие шифры законных пользователей.
- разработка и распространение компьютерных вирусов. Программы-вирусы обладают свойствами переходить через коммуникационные сети из одной системы в другую, распространяясь как вирусное заболевание;
- ввод в программное обеспечение «логических бомб». Это такие программы, которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему;
- халатная небрежность при разработке, создании и эксплуатации программно-вычислительных комплексов компьютерных сетей, приведшая к тяжким последствиям. Особенностью компьютерных систем является то, что абсолютно безошибочных программ в принципе не бывает. Если проект практически в любой области техники можно выполнить с огромным запасом

надежности, то в области программирования такая надежность весьма условна, а в ряде случаев почти недостижима;

- подделка и фальсификация компьютерной информации. По-видимому, этот вид компьютерной преступности является одним из наиболее распространенных. Он представляет собой разновидность несанкционированного доступа с той лишь разницей, что пользоваться им может сам разработчик, причем имеющий достаточно высокую квалификацию. Идея преступления состоит в подделке выходной информации с целью имитации работоспособности больших систем, составной частью которых является компьютер. При достаточно ловко выполненной подделке зачастую удается сдать заказчику заведомо неисправную продукцию.
- хищение программного обеспечения. Если «обычные» хищения подпадают под действие существующего уголовного закона, то проблема хищения программного обеспечения значительно более сложна. Значительная часть программного обеспечения в России распространяется путем кражи и обмена краденым;
- несанкционированное копирование, изменение или уничтожение информации. При неправомерном обращении в собственность машинная информация может не изыматься из фондов, а копироваться. Следовательно, машинная информация должна быть выделена как самостоятельный предмет уголовно-правовой охраны;
- несанкционированный просмотр или хищение информации из банков данных, баз данных и баз знаний. В данном случае под базой данных следует понимать форму представления и организации совокупности данных (например: статей, расчетов), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ.

Приходится констатировать, что процесс компьютеризации общества приводит к увеличению количества компьютерных преступлений, возрастанию их удельного веса в общей доле материальных потерь от различных видов преступлений.

Парадоксальная особенность компьютерных преступлений состоит и в том, что трудно найти другой вид преступления, после совершения которого его жертва не выказывает особой заинтересованности в поимке преступника, а сам преступник, будучи пойман, всячески рекламирует свою деятельность на поприще компьютерного взлома, мало что утаивая от представителей правоохранительных органов. Психологически этот парадокс вполне объясним.

Во-первых, жертва компьютерного преступления совершенно убеждена, что затраты на его раскрытие (включая потери, понесенные в результате утраты своей репутации) существенно превосходят уже причиненный ущерб.

И, во-вторых, преступник приобретает широкую известность в деловых и криминальных кругах, что в дальнейшем позволяет ему с выгодой использовать приобретенный опыт.

Важнейшим и определяющим элементом криминалистической характеристики любого, в том числе и компьютерного, преступления является совокупность данных, характеризующих способ его совершения.

Под способом совершения преступления обычно понимают объективно и субъективно обусловленную систему поведения субъекта до, в момент и после совершения преступления, которое оставляет различного рода характерные следы, позволяющие с помощью криминалистических приемов и средств получить представление о сути происшедшего, своеобразии преступного поведения правонарушителя, его отдельных личностных данных и, соответственно, определить оптимальные методы решения задач раскрытия преступления.

Способы совершения компьютерных преступлений:

- изъятие средств компьютерной техники;
- перехват информации;
- несанкционированный доступ;
- манипуляция данными и управляющими командами;
- комплексные методы.

К первой группе относятся традиционные способы совершения обычных видов преступлений, в которых действия преступника направлены на изъятие чужого имущества. Характерной отличительной чертой данной группы способов совершения компьютерных преступлений является тот факт, что в них средства компьютерной техники всегда выступают только в качестве предмета преступного посягательства. Например, прокуратурой г. Кургана в 1997 г. расследовалось уголовное дело по факту убийства частного предпринимателя. В ходе обыска на квартире убитого следователем был изъят персональный компьютер. По имеющейся оперативной информации в памяти компьютера убитый мог хранить фамилии, адреса своих кредиторов и должников. В дальнейшем этот компьютер по решению следователя был передан в одну из компьютерных фирм для производства исследования содержимого его дисков памяти. В ту же ночь из

помещения упомянутой компьютерной фирмы путем отгиба решеток была произведена кража данного компьютера. В результате того, что изъятие и передача ЭВМ были произведены следователем с рядом процессуальных нарушений, данное преступление осталось нераскрытым.

Ко второй группе относятся способы совершения компьютерных преступлений, основанные на действиях преступника, направленных на получение данных и машинной информации посредством использования методов аудиовизуального и электромагнитного перехвата.

Активный перехват осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера, например линии принтера или телефонному проводу канала связи либо непосредственно через соответствующий порт персонального компьютера.

Пассивный (электромагнитный) перехват основан на фиксации электромагнитных излучений, возникающих при функционировании многих средств компьютерной техники, включая и средства коммуникации. Так, например, излучение электронно-лучевой трубки дисплея можно принимать с помощью специальных приборов на расстоянии до 1000 м.

Аудиоперехват или снятие информации по виброакустическому каналу является опасным и достаточно распространенным способом и имеет две разновидности. А) установка подслушивающего устройства в аппаратуру средств обработки информации. Б) установка микрофона на инженерно-технические конструкции за пределами охраняемого помещения (стены, оконные рамы, двери и т.п.).

Видеоперехват осуществляется путем использования различной видеооптической техники.

«Уборка мусора» представляет собой достаточно оригинальный способ перехвата информации. Преступником неправомерно используются технологические отходы информационного процесса, оставленные пользователем после работы с компьютерной техникой. Например, даже удаленная из памяти и с жестких дисков компьютера, а также с дискет информация может быть восстановлена и несанкционированно изъята с помощью специальных программных средств.

К третьей группе способов совершения компьютерных преступлений относятся действия преступника, направленные на получение несанкционированного доступа к информации. В эту группу входят следующие способы.

«Компьютерный абордаж» — несанкционированный доступ в компьютер или компьютерную сеть без права на то. Этот способ используется хакерами для проникновения в чужие информационные сети.

Преступление осуществляется чаще всего путем случайного перебора абонентного номера компьютерной системы с использованием модемного устройства. Иногда для этих целей используется специально созданная программа автоматического поиска пароля. Алгоритм ее работы заключается в том, чтобы, учитывая быстродействие современных компьютеров, перебирать все возможные варианты комбинаций букв, цифр и специальных символов и в случае совпадения комбинаций символов производить автоматическое соединение указанных абонентов.

Эксперименты по подбору пароля путем простого перебора показали, что 6-символьные пароли подбираются примерно за 6 дней непрерывной работы компьютера. Элементарный подсчет свидетельствует о том, что уже для подбора 7-символьных паролей потребуется от 150 дней для английского языка и до 200 дней для русского. А если учитывать регистр букв, то эти числа надо умножить еще на 2. Таким образом, простой перебор представляется чрезвычайно трудновыполнимым.

Поэтому в последнее время преступниками стал активно использоваться метод «интеллектуального перебора», основанный на подборе предполагаемого пароля, исходя из заранее определенных тематических групп его принадлежности. В этом случае программе-взломщику передаются некоторые исходные данные о личности автора пароля. По оценкам специалистов, это позволяет более чем на десять порядков сократить количество возможных вариантов перебора символов и на столько же — время на подбор пароля.

«За дураком». Этот способ используется преступником путем подключения компьютерного терминала к каналу связи через коммуникационную аппаратуру в тот момент времени, когда сотрудник, отвечающий за работу средства компьютерной техники, кратковременно покидает свое рабочее место, оставляя терминал в активном режиме.

«За хвост». При этом способе съема информации преступник подключается к линии связи законного пользователя и дожидается сигнала, обозначающего конец работы, перехватывает его и осуществляет доступ к системе.

«Неспешный выбор». При данном способе совершения преступления преступник осуществляет несанкционированный доступ к компьютерной системе путем нахождения слабых мест в ее защите.

Этот способ чрезвычайно распространен среди хакеров. В интернете и других глобальных компьютерных сетях идет постоянный поиск, обмен, покупка и продажа взломанных хакерами программ. Существуют специальные телеконференции, в которых проходит обсуждение программ-взломщиков, вопросов их создания и распространения.

«Брешь». В отличие от «неспешного выбора», когда производится поиск уязвимых мест в защите компьютерной системы, при данном способе преступником осуществляется конкретизация поиска: ищутся участки программ, имеющие ошибку или неудачную логику построения. Выявленные таким образом «бреши» могут использоваться преступником многократно, пока не будут обнаружены законным пользователем.

«Люк». Данный способ является логическим продолжением предыдущего. В месте найденной «бреши» программа «разрывается» и преступником туда дополнительно вводится одна или несколько команд. Такой «люк» «открывается» по необходимости, а включенные команды автоматически выполняются.

Люки часто бывают оставлены самими создателями программ, иногда с целью внесения возможных изменений. Подобные «черные входы» в защищенную систему обычно имеются в любой сертифицированной программе, но об этом не принято распространяться вслух.

К четвертой группе способов совершения компьютерных преступлений относятся действия преступников, связанные с использованием методов манипуляции данными и управляющими командами средств компьютерной техники. Эти методы наиболее часто используются преступниками для совершения различного рода противоправных деяний.

Наиболее часто встречаются следующие способы совершения компьютерных преступлений, относящихся к этой группе:

«Троянский конь». Данный способ заключается в тайном введении в чужое программное обеспечение специально созданных программ, которые, попадая в информационно-вычислительные системы, начинают выполнять новые, не планировавшиеся законным владельцем действия, с одновременным сохранением

прежних функций. В соответствии со ст. 273 Уголовного кодекса Российской Федерации под такой программой понимается «программа для ЭВМ, приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети». По существу, «троянский конь» — это модернизация рассмотренного выше способа «люк» с той лишь разницей, что люк «открывается» не при помощи непосредственных действий преступника, а автоматически, с использованием специально подготовленной для этих целей программы и без непосредственного участия самого преступника. С помощью такого способа преступники обычно отчисляют на заранее открытый счет определенную сумму с каждой банковской операции. Возможен и вариант увеличения преступниками избыточных сумм на счетах при автоматическом пересчете рублевых остатков, связанных с переходом к коммерческому курсу соответствующей валюты.

Компьютерный вирус. С уголовно-правовой точки зрения, согласно ст. 273 Уголовного кодекса РФ, под компьютерным вирусом следует понимать вредоносную для ЭВМ программу, способную самопроизвольно присоединяться к другим программам («заражать» их) и при запуске последних выполнять различные нежелательные действия: порчу файлов, искажение, стирание данных и информации, переполнение машинной памяти и создание помех в работе ЭВМ.

Компьютерное мошенничество чаще всего осуществляется способом «подмены данных» или «подмены кода. Это наиболее простой и поэтому очень часто применяемый способ совершения преступления. Действия преступников в этом случае направлены на изменение или введение новых данных, и осуществляются они, как правило, при вводе-выводе информации. Некоторые из таких способов совершения преступлений возникли и получили распространение только с появлением компьютеров. В качестве примера можно привести перебрасывание на подставной счет мелочи, являющейся результатом округления (операция типа «салями»). Расчет построен на том, что компьютер совершает сотни тысяч операций в секунду и обрабатывает при этом сотни тысяч счетов клиентов. Заниматься подобным мошенничеством вручную не имеет никакого смысла.

Незаконное копирование (тиражирование) программ с преодолением программных средств защиты предусматривает незаконное создание копии ключевой дискеты, модификацию кода системы защиты, моделирование обращения к ключевой дискете, снятие системы защиты из памяти ЭВМ и т.п.

Пятая группа способов — комплексные методы — включает в себя различные комбинации рассмотренных выше способов совершения компьютерных преступлений.

Следует заметить, что рассмотренная выше классификация не является единственно возможной. Так, по международной классификации в отдельную группу принято выделять такие способы, как компьютерный саботаж с аппаратным или программным обеспечением, которые приводят к выходу из строя компьютерной системы. Наиболее значительные компьютерные преступления совершаются посредством порчи программного обеспечения, причем часто его совершают работники, недовольные своим служебным положением, отношениями с руководством и т.д.

Примером такого компьютерного преступления может служить получивший широкую огласку случай с программистом, остановившим главный конвейер Волжского автозавода в г. Тольятти. Занимаясь отладкой программного кода автоматизированной системы, управляющей подачей механических узлов на конвейер, он умышленно внес изменения в программу. В результате, после прохождения заданного числа деталей система «зависала» и конвейер останавливался. Пока программисты устраняли источник сбоев, с конвейера автозавода сошло не более двухсот машин.

Существует также ряд способов совершения преступлений, которые крайне сложно отнести к какой либо группе. К таким способам относятся асинхронная атака, моделирование, мистификация, маскарад и т.д.

Асинхронная атака. Сложный способ, требующий хорошего знания операционной системы. Используя асинхронную природу функционирования большинства операционных систем, их заставляют работать при ложных условиях, из-за чего управление обработкой информации частично или полностью нарушается. Если лицо, совершающее «асинхронную атаку», достаточно профессионально, оно может использовать ситуацию, чтобы внести изменения в операционную систему или сориентировать ее на выполнение своих целей, причем извне эти изменения не будут заметны.

Моделирование. Создается модель конкретной системы, в которую вводятся исходные данные и учитываются планируемые действия. На основании полученных результатов методом компьютерного перебора и сортировки выбираются возможные подходящие комбинации. Затем модель возвращается к исходной точке

и выясняется, какие манипуляции с входными данными нужно проводить для получения на выходе желаемого результата. В принципе, «прокручивание» модели вперед-назад может происходить многократно, чтобы через несколько итераций добиться необходимого итога. После этого остается осуществить задуманное на практике.

Мистификация. Возможна, например, в случаях, когда пользователь удаленного терминала ошибочно подключается к какой-либо системе, будучи абсолютно уверенным, что работает именно с той самой системой, с которой намеревался. Владелец системы, к которой произошло подключение, формируя правдоподобные отклики, может поддержать контакт в течение определенного времени и получать конфиденциальную информацию, в частности коды пользователя и т.д.

Мотивами совершения компьютерных преступлений, как показали исследования зарубежных и российских исследователей, являются следующие:

- корыстные соображения — 66,%;
- политические цели — 17%;
- исследовательский интерес — 7%;
- хулиганство — 5%;
- месть — 5%.

1.5. Ущерб от нарушения информационной безопасности и последствия данного ущерба

Ущерб данным можно условно разделить на два типа, это:

- Раскрытие информации.
- Искажение и уничтожение информации.

Раскрытие данных предполагает, что кому-то случайно или после целенаправленных действий стал известен смысл информации.

Этот вид нарушения встречается наиболее часто. Последствия могут быть самые разные. Очень важную информацию, тщательно оберегаемую от раскрытия, представляют сведения о людях: истории болезни, письма, состояния счетов в банках.

Обычно данные о людях наиболее важны для них самих, но, как бы это не описывали в шпионских фильмах, мало что значат для похитителей. Иногда личные данные могут использоваться для компрометации не только отдельных людей, но

целых организаций, например, если выяснится скрываемая прежняя судимость за растрату директора коммерческого банка.

Основной убыток от разглашения информации - личное несчастье человека. Другое дело - раскрытие стратегической управляющей информации. Если вскрыт долгосрочный план развития производства или анализ конъюнктуры на рынке, то потери для держателя этой информации будут невелики, но для конкурентов такие сведения очень важны.

Искажения или уничтожение информации представляют существенно большую опасность. Во многих организациях жизненно важные данные хранятся в файлах: инвентарные описи, графики работ, списки заказов. Если такие данные будут искажены или стерты, то работа надолго парализуется.

Таким образом можно скомпрометировать бухгалтерскую или конструкторскую систему, чуть исказив десяток-другой чисел, или удалить сведения о реальном движении товара, чтобы счет за него не был выставлен. Похоже, что наиболее уязвима для искажения информация экономического характера, где потери могут быть чрезвычайно велики.

Возможные последствия ущерба информационной безопасности:

- нарушение конституционных прав на сохранение личной тайны и конфиденциальности персональных данных;
- экономический и моральный ущерб вследствие разглашения коммерческой тайны или «электронного мошенничества»;
- аварии на железнодорожном и воздушном транспорте вследствие нарушения работы систем управления ими;
- экологические катастрофы; ущерб в политической или военной сфере вследствие разглашения государственной тайны.

и многие другие...

Глава 2. Защита информации

2.1. Методы защиты информации

Постепенно, по мере формирования системного подхода к проблеме обеспечения безопасности данных, возникла необходимость комплексного применения методов

защиты и созданных на их основе средств и механизмов защиты. Кратко рассмотрим основные методы защиты данных.

Управление представляет собой регулирование использования всех ресурсов системы в рамках установленного технологического цикла обработки и передачи данных, где в качестве ресурсов рассматриваются технические средства, операционные системы, программы, базы данных и элементы данных.

Препятствия физически преграждают нарушителю путь к защищаемым данным. Организация защиты информации основывается на четырех уровнях защиты: правовом, административном, аппаратно-программном, криптографическом.

Маскировка представляет собой метод защиты данных путем их криптографического закрытия.

Регламентация как метод защиты заключается в разработке и реализации комплексов мероприятий, создающих такие условия технологического цикла обработки данных, при которых минимизируется риск несанкционированного доступа к данным. Регламентация охватывает как структурное построение информационной системы, так и технологию обработки данных, организацию работы пользователей и персонала сети.

Побуждение состоит в создании такой обстановки и условий, при которых правила обращения с защищенными данными регулируются моральными и нравственными нормами.

Принуждение включает угрозу материальной, административной и уголовной ответственности за нарушение правил обращения с защищенными данными.

2.2. Средства защиты информации

На основе перечисленных методов создаются средства защиты данных. Все средства защиты данных можно разделить на формальные и неформальные.

Формальными называются такие средства защиты, которые выполняют свои функции по заранее установленным процедурам без вмешательства человека. К формальным средствам защиты относятся технические и программные средства.

К техническим средствам защиты относятся все устройства, которые предназначены для защиты данных. В свою очередь, технические средства защиты можно разделить на физические и аппаратные.

Физические средства защиты создают препятствия для нарушителей на путях к защищаемым данным, например, на территорию, на которой располагаются объекты ИВС, в помещения с аппаратурой, носителями данных и т.п.

Физические средства защиты выполняют следующие основные функции:

- охрана территории и зданий;
- охрана внутренних помещений;
- охрана оборудования и наблюдение за ним;
- контроль доступа в защищаемые зоны;
- нейтрализация излучений и наводок;
- создание препятствий визуальному наблюдению и подслушиванию;
- противопожарная защита;
- блокировка действий нарушителя и т.п.

Для предотвращения проникновения нарушителей на охраняемые объекты применяются следующие технические устройства:

сверхвысокочастотные, ультразвуковые и инфракрасные системы;

- лазерные и оптические системы;
- телевизионные (ТВ) системы;
- кабельные системы;
- системы защиты окон и дверей.

Под аппаратными средствами защиты понимаются специальные средства, непосредственно входящие в состав технического обеспечения ИВС и выполняющие функции защиты как самостоятельно, так и в комплексе с другими средствами.

Аппаратные средства защиты данных можно условно разбить на группы согласно типам аппаратуры, в которых они используются. В качестве таких групп рассмотрим следующие:

- средства защиты процессора;
- средства защиты памяти;
- средства защиты терминалов;
- средства защиты устройств ввода-вывода;
- средства защиты каналов связи

Программными называются средства защиты данных, функционирующие в составе программного обеспечения средств и механизмов защиты данных. Они выполняют функции защиты данных самостоятельно или в комплексе с другими средствами защиты.

Рассмотрим классификацию программных средств защиты по функциональному назначению:

- Средства внешней защиты (защита каналов связи, защита территории, защита помещений, защита устройств информационной системы)
- Средства внутренней защиты (защита операционных систем, программного обеспечения, баз данных)
- Средства управления защитой (регистрация пользователей, распределение ресурсов, идентификация и установление подлинности)
- Средства обеспечения защиты (контроль, генерация служебной информации, сигнализация, рассылка информации о защите пользователям, компенсация нарушений функционирования, координация работы системы обеспечения безопасности)

Отдельную группу формальных средств составляют криптографические средства, которые реализуются в виде программных, аппаратных и программно-аппаратных средств защиты.

Неформальными называются такие средства защиты, которые реализуются в результате деятельности людей, либо регламентируют эту деятельность.

Неформальные средства включают организационные, законодательные и морально-этические меры и средства.

Под организационными средствами защиты понимаются организационно-технические и организационно-правовые мероприятия, осуществляемые для обеспечения безопасности данных.

Мероприятия, осуществляемые при создании сети, обеспечивают выполнение требований защиты:

- при разработке системы в целом и всех ее подсистем;
- при монтаже и наладке оборудования;
- при разработке математического, программного, информационного и технического обеспечения сети;

- при испытаниях и приемке сети в эксплуатацию.

Мероприятия, осуществляемые в процессе эксплуатации сети включают в себя:

- организацию пропускного режима; организацию технологического цикла обработки и передачи данных;
- организацию работы обслуживающего персонала;
- организацию интерфейса пользователей с сетью;
- организацию ведения протоколов обмена;
- распределение реквизитов разграничения доступа между пользователями (паролей, профилей полномочий, списков доступа и т.п.).

Мероприятия общего характера включают в себя:

- учет требований защиты при подборе и подготовке кадров;
- организацию плановых и внезапных проверок функционирования механизмов защиты;
- планирование всех мероприятий по обеспечению безопасности данных:
- разработку документов по обеспечению безопасности данных и т.д.

Рассмотрим основные принципы организации работ, которые способствуют обеспечению безопасности данных:

Минимизация сведений, доступных персоналу. Этот принцип означает, что каждый сотрудник должен знать только те детали процесса обеспечения безопасности данных, которые необходимы ему для выполнения своих обязанностей.

Минимизация связей персонала. Организация технологического цикла сбора, обработки и передачи данных, по мере возможности, должна исключать или минимизировать контакты обслуживающего персонала.

Разделение полномочий. В системах с высокими требованиями по обеспечению безопасности данных ответственные процедуры выполняются, как правило, после подтверждения их необходимости двумя сотрудниками.

Минимизация доступных данных требует ограничения количества данных, которые могут быть доступны персоналу и пользователям.

Дублирование контроля. Контроль важнейших операций нельзя поручать одному сотруднику.

Ведение эксплуатационной документации подразумевает фиксацию факта передачи смены с перечислением того, что и в каком состоянии передается. Особенности организации обеспечения безопасности данных отражаются в эксплуатационной документации и функциональных обязанностях персонала, которые разрабатываются с учетом целей и задач, стоящих перед сетью, и требований по защите данных в ней.

В системах с повышенными требованиями к защите вводится специальное должностное лицо, занимающееся вопросами обеспечения безопасности данных.

Негативным последствием информатизации общества является и появление компьютерных преступлений.

Законодательные меры позволяют сдерживать потенциальных преступников, причем под законодательными мерами понимаются законодательные акты, которыми регламентируются правила использования данных ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

Основы такого законодательства заложены в Декларации прав и свобод гражданина, принятых Верховным Советом РФ 12 ноября 1991 года. Пункт 2 статьи 13 этой декларации гласит: "Каждый человек имеет право искать, получать и свободно распространять информацию. Ограничения этого права могут устанавливаться Законом только в целях охраны личной, семейной, профессиональной, коммерческой и государственной тайны, а также нравственности".

Данное положение дает основу для построения иерархии законов. Важнейшим из них является Закон "О государственной тайне", вступивший в действие 21 сентября 1993 года. Согласно этому закону под государственной тайной понимаются защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ. Необходимо отметить, что данный Закон не рассматривает человека в качестве носителя сведений, составляющих государственную тайну.

Закон о государственной тайне устанавливает органы защиты государственной тайны, к которым относятся:

- межведомственная комиссия по защите государственной тайны;

- органы федеральной исполнительной власти (Министерства безопасности и обороны, Федеральное Агентство Правительственной Связи и Информации), служба внешней разведки, Государственная техническая комиссия (ГТК) и их органы на местах;
- органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите государственной тайны.

К морально-этическим нормам защиты относятся всевозможные нормы, которые традиционно сложились или складываются по мере развития информатизации общества. Такие нормы не являются обязательными, однако, их несоблюдение ведет, как правило, к потере авторитета, престижа человека, группы лиц или целой организации. Считается, что этические нормы оказывают положительное воздействие на персонал и пользователей.

Морально-этические нормы могут быть неписанными (например, общепринятые нормы честности, патриотизма и т.п.) и оформленными в качестве свода правил и предписаний (кодексов).

Заключение

Спектр использования злоумышленниками уязвимостей информационных систем с течением времени лишь увеличивается. Это закономерно приводит к тому, что промышленные компании должны выделять больше сил и средств на защиту своей информации, ведь в противном случае потери могут быть слишком велики.

Если раньше эти функции выполняли обычные IT специалисты, то сейчас ситуация поменялась. Все больше компаний хотят иметь в своем штате хорошего специалиста в этой области.

Именно поэтому изучение всех аспектов информационной безопасности очень важно при подготовке специалистов информационного звена в наше время.

В данной работе мы рассмотрели понятие и общие принципы информационной безопасности, потенциальные источники угроз информации, а так же средства защиты информации. Разумеется, этот материал — лишь фундамент для более углубленного изучения информационной безопасности.

Помимо того, что, как было сказано во введении, защита информации должна быть непрерывным процессом, непрерывным процессом должно быть и изучение ёе составляющих, ведь эта наука, будучи совсем молодой, постоянно преподносит своим исследователям новые открытия.

Список использованной литературы

1. Блинов А.М. Информационная безопасность: Учебное пособие. Часть 1. – СПб.: Изд-во СПбГУЭФ, 2010. – 96 с.
2. Петренко С.А., Курбатов В.А. – Политики безопасности компании при работе в интернет (Информационные технологии для инженеров) – Москва.: ДМК-Пресс, 2011. – 302 с.
3. Юрий Родичев. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. – СПб.: Изд-во Питер, 2017. – 256 с.
4. Елена Баранова, Александр Бабаш. Информационная безопасность и защита. Учебное пособие. – Москва.: РИОР, 2017. – 324 с.