Безопасность информации и ее правовое обеспечение, компьютерные преступления

План занятия

1. Понятия «компьютерное преступление» и «информационная безопасность».
2. Виды компьютерных преступлений.
3. Способы и методы предупреждения компьютерных преступлений.
4. Компьютерные вирусы, их классификация и поражающие особенности.
5. Методы защиты информации при использовании компьютерных сетей.
6. Метод «интеллектуального перебора паролей».
7. Правовое обеспечение информационной безопасности.

Информационная безопасность – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

Признаки

Информация с точки зрения информационной безопасности обладает следующими **категориями** - конфиденциальность, целостность, аутентичность и апелируемость.

Конфиденциальность - гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена. Нарушение этой категории называется хищением или раскрытием информации.

Целостность - гарантия того, что информация сейчас существует в ее исходном виде, при ее хранении или передаче не было произведено несанкционированных изменений. Нарушение этой категории называется фальсификацией сообщения.

Аутентичность - гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор. Нарушение этой категории называется фальсификацией автора сообщения.

Апеллируемость - часто применяемая в электронной коммерции - гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно заявленный человек. Отличие этой категории от предыдущей в том, что при подмене автора кто-то пытается заявить, что он автор сообщения, а при нарушении апеллируемости сам автор пытается отказаться от слов, подписанных им.

Задачи

Основными задачами являются:

- обеспечение контроля и надзора, разрешительной и регистрационной деятельности в сфере связи, информационных технологий и массовых коммуникаций;

- обеспечение безопасности функционирования информационных и телекоммуникационных систем;

- развитие технологий защиты информации, обеспечивающих неприкосновенность частной жизни, личной и семейной тайны, безопасность информации ограниченного доступа;

- противодействие распространению идеологии терроризма, экстремизма, пропаганды насилия.

Угрозы информационной безопасности

Угрозы информационной безопасности могут быть разделены на два вида:

естественные угрозы физических воздействий на информацию стихийных природных явлений – угрозы не зависящие от деятельности человека;

искусственные угрозы – угрозы, вызванные человеческой деятельностью и являющиеся гораздо более опасными.

Искусственные угрозы, в зависимости от их мотивов, разделяются на *непреднамеренные* (случайные) и *преднамеренные* (умышленные).

К непреднамеренным угрозам относятся:

- ошибки в проектировании КС;
- ошибки в разработке программных средств КС;
- случайные сбои в работе аппаратных средств КС, линий связи, энергоснабжения;
- ошибки пользователей КС;
- воздействие на аппаратные средства КС физических полей других электронных устройств (при несоблюдении условий их электромагнитной совместимости) и др.

Компьютерное преступление - любое противоправное действие, при котором компьютер выступает либо как объект, против которого совершается преступление, либо как инструмент, используемый для совершения преступных действий.

Виды

Несанкционированный доступ и перехват

- компьютерный абордаж
- перехват
- кража времени
- прочие виды несанкционированного доступа и перехвата

Изменение компьютерных данных

- логическая бомба
- троянский конь
- компьютерный вирус
- компьютерный червь
- прочие виды изменения данных

Компьютерное мошенничество
- мошенничество с банкоматами
- компьютерная подделка
- мошенничество с игровыми автоматами
- манипуляции с программами ввода-вывода
- мошенничества с платежными средствами
- телефонное мошенничество
- прочие компьютерные мошенничества

Незаконное копирование
- компьютерные игры
- прочее программное обеспечение
- топография полупроводниковых изделий
- прочее незаконное копирование

Компьютерный саботаж
- с аппаратным обеспечением
- с программным обеспечением
- прочие виды саботажа

Прочие компьютерные преступления

- с использованием компьютерных досок объявлений
- хищение информации, составляющей коммерческую тайну
- передача информации конфиденциального характера
- прочие компьютерные преступления

Способы и методы предупреждения компьютерных преступлений

Методика предупреждения преступлений является важной составной частью методологии криминалистики и включается в общее понятие методики борьбы с отдельными видами преступлений, к которым относятся и компьютерные преступления.

Между тем многие работники органов внутренних дел и прежде всего следственных аппаратов, непосредственно осуществляющих борьбу с преступностью, слабо подготовлены профессионально для осуществления достаточно трудоемких и сложных мероприятий по предупреждению компьютерных преступлений.

Это в значительной степени обусловлено тем, что в настоящее время не существует сколько-нибудь конкретных и полных по содержанию методологических разработок по организации и тактике предупреждения преступлений рассматриваемой категории. Надо принять во внимание и специфичность и новизну компьютерных преступлений, выраженных, в частности, в повышенной трудности их выявления, раскрытия и расследования.

На основе данных, полученных в ходе анализа отечественной и зарубежной специальной литературы и публикаций в периодической печати по вопросам теории и практики борьбы с компьютерной преступностью, можно выделить три основные *группы мер предупреждения компьютерных преступлений*:

1) правовые;
2) организационные;
3) технические.

К **правовым** мерам следует отнести:

· разработку норм, устанавливающих ответственность за компьютерные преступления,

· защиту авторских прав программистов,

· совершенствование уголовного и гражданского законодательства, а также судопроизводства.

К **организационным** мерам относят:

· охрану вычислительного центра;

· тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком;

· наличие плана восстановления работоспособности центра после выхода его из строя;

· организацию обслуживания вычислительного центра посторонней организацией или лицами, не заинтересованными в сокрытии фактов нарушения работы центра;

· универсальность средств защиты от всех пользователей (включая высшее руководство);

· возложение ответственности на лиц, которые должны обеспечить безопасность центра, выбор места расположения центра и т.п.

К **техническим** мерам можно отнести:

· защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем;

· организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев;

· установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды;·

· принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов;

· установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

Рассмотрим их более подробно.

К **правовым мерам** предупреждения компьютерных преступлений в первую очередь относятся нормы законодательства, устанавливающие уголовную ответственность за указанные выше противоправные деяния.

История развития законодательства зарубежных стран в этом направлении показывает, что впервые подобный шаг был предпринят законодательными собраниями американских штатов Флорида и Аризона уже в 1978 году. Принятый закон назывался “Computer crime act of 1978” и был первым в мире специальным законом, устанавливающим уголовную ответственность за компьютерные преступления. Затем практически во всех штатах США (в 45 штатах) были приняты аналогичные специальные законодательства.

Эти правовые акты стали фундаментом для дальнейшего развития законодательства в целях осуществления мер предупреждения компьютерных преступлений.

Отечественное законодательство движется в этом направлении очень робкими шагами.

Первым из них по праву можно считать издание 22 октября 1992 года двух Указов Президента РФ “О правовой охране программ для ЭВМ и баз данных” и “О правовой охране топологий интегральных микросхем”, регламентирующих порядок установления и правовую защиту авторских прав на программные средства компьютерной техники (СКТ) и топологии интегральных микросхем с 1 января 1994 года.

Вторым прогрессивным шагом является принятие Государственной Думой и Федеральным Собранием сразу двух законов: 20 января - “О связи” и 25 января 1995 г. “Об информации, информатизации и защите информации”. Данные нормативные акты дают юридическое определение основных компонентов информационной технологии как объектов правовой охраны; устанавливают и закрепляют права и обязанности собственника на эти объекты; определяют правовой режим функционирования средств информационных технологий; определяют категории доступа определенных субъектов к конкретным видам информации; устанавливают категории секретности данных и информации.

Решающим законодательным шагом можно считать принятие в июне 1996 года Уголовного Кодекса Российской Федерации и выделяющего информацию в качестве объекта уголовно-правовой охраны.

Организационные меры защиты СКТ включают в себя совокупность организационных мероприятий: по подбору, проверке и инструктажу персонала; разработке плана восстановления информационных объектов после входа их из строя; организации программно-технического обслуживания СКТ; возложению дисциплинарной ответственности на лиц по обеспечению безопасности конкретных СКТ; осуществлению режима секретности при функционировании компьютерных систем; обеспечению режима физической охраны объектов; материально-техническому обеспечению и т.д.

Организационные меры являются важным и одним из эффективных средств защиты информации, одновременно являясь фундаментом, на котором строится в дальнейшем вся система защиты.

Анализ материалов отечественных уголовных дел позволяет сделать вывод о том, что основными причинами и условиями, способствующими совершению компьютерных преступлений в большинстве случаев стали:

1) неконтролируемый доступ сотрудников к клавиатуре компьютера, используемого как автономно, так и в качестве рабочей станции автоматизированной сети для дистанционной передачи данных первичных бухгалтерских документов в процессе осуществления финансовых операций;

2) бесконтрольность за действиями обслуживающего персонала, что позволяет преступнику свободно использовать ЭВМ в качестве орудия совершения преступления;

3) низкий уровень программного обеспечения, которое не имеет контрольной защиты, обеспечивающей проверку соответствия и правильности вводимой информации;

4) несовершенство парольной системы защиты от несанкционированного доступа к рабочей станции и ее программному обеспечению, которая не обеспечивает достоверную идентификацию пользователя по индивидуальным биометрическим параметрам;

5) отсутствие должностного лица, отвечающего за режим секретности и конфиденциальности коммерческой информации;

6) отсутствие категорийности допуска сотрудников к документации строгой финансовой отчетности;

7) отсутствие договоров (контрактов) с сотрудниками на предмет неразглашения коммерческой и служебной тайны, персональных данных и иной конфиденциальной информации.

Для эффективной безопасности от компьютерных преступлений всего лишь необходимо:

1) просмотреть всю документацию в учреждении, организации;

2) ознакомиться с функциями и степенью ответственности каждого сотрудника;

3) определить возможные каналы утечки информации;

4) ликвидировать обнаруженные слабые звенья в защите.

Зарубежный опыт показывает, что наиболее эффективной мерой в этом направлении является введение в штатное расписание организации должности специалиста по компьютерной безопасности (администратора по защите информации) либо создание специальных служб как частных, так и централизованных, исходя из конкретной ситуации. Наличие такого отдела (службы) в организации снижает вероятность совершения компьютерных преступлений вдвое.

Кроме этого, в обязательном порядке должны быть реализованы следующие организационные мероприятия:

1) для всех лиц, имеющих право доступа к СКТ, должны быть определены категории допуска;

2) определена административная ответственность для лиц за сохранность и санкционированность доступа к имеющимся информационным ресурсам;

3) налажен периодический системный контроль за качеством защиты информации посредством проведения регламентных работ как самим лицом, ответственным за безопасность, так и с привлечением специалистов;

4) проведена классификация информации в соответствии с ее важностью;

5) организована физическая защита СКТ (физическая охрана).

Меры технического характера. Условно их можно подразделить на три основные группы в зависимости от характера и специфики охраняемого объекта, а именно: аппаратные, программные и комплексные.

Аппаратные методы предназначены для защиты аппаратных средств и средств связи компьютерной техники от нежелательных физических воздействий на них сторонних сил, а также для закрытия возможных нежелательных каналов утечки конфиденциальной информации и данных, образующихся за счет побочных электромагнитных излучений и наводок, виброакустических сигналов, и т.п.

Практическая реализация данных методов обычно осуществляется с помощью применения различных технических устройств специального назначения. К ним, в частности, относятся:

1) источники бесперебойного питания, предохраняющие от скачкообразных перепадов напряжения;

2) устройства экранирования аппаратуры, линий проводной связи и помещений, в которых находятся СКТ;

3) устройства комплексной защиты телефонии;

4) устройства, обеспечивающие только санкционированный физический доступ пользователя на охраняемые объекты СКТ (шифрозамки, устройства идентификации личности и т.п.);

5) устройства идентификации и фиксации терминалов и пользователей при попытках несанкционированного доступа к компьютерной сети;

6) средства охранно-пожарной сигнализации;

7) средства защиты портов компьютерной техники (наиболее эффективны для защиты компьютерных сетей от несанкционированного доступа) и т.д.

Программные методы защиты предназначаются для непосредственной защиты информации по трем направлениям: а) аппаратуры; б) программного обеспечения; в) данных и управляющих команд.

Для защиты информации при ее передаче обычно используют различные **методы шифрования** данных перед их вводом в канал связи или на физический носитель с последующей расшифровкой. Как показывает практика, методы шифрования позволяют достаточно надежно скрыть смысл сообщения.

Все **программы** защиты, осуществляющие **управление доступом** к машинной информации, функционируют по принципу ответа на вопросы: кто может выполнять, какие операции и над какими данными.

Доступ может быть определен как:

- общий (безусловно предоставляемый каждому пользователю);
- отказ (безусловный отказ, например разрешение на удаление порции информации);
- зависимый от события (управляемый событием);
- зависимый от содержания данных;
- зависимый от состояния (динамического состояния компьютерной системы);
- частотно-зависимый (например, доступ разрешен пользователю только один или определенное число раз);
- по имени или другим признаком пользователя;
- зависимый от полномочий;
- по разрешению (например, по паролю);
- по процедуре.

Также к эффективным мерам противодействия попыткам несанкционированного доступа относятся **средства регистрации**. Для этих целей наиболее перспективными являются новые операционные системы специального назначения, широко применяемые в зарубежных странах и получившие название **мониторинга** (автоматического наблюдения за возможной компьютерной угрозой).

Мониторинг осуществляется самой операционной системой (ОС), причем в ее обязанности входит контроль за процессами ввода-вывода, обработки и уничтожения машинной информации. ОС фиксирует время несанкционированного доступа и программных средств, к которым был осуществлен доступ. Кроме этого, она производит немедленное оповещение службы компьютерной безопасности о посягательстве на безопасность компьютерной системы с одновременной выдачей на печать необходимых данных (листинга).

В последнее время в США и ряде европейских стран для защиты компьютерных систем действуют также специальные подпрограммы, вызывающие самоуничтожение основной программы при попытке несанкционированного просмотра содержимого файла с секретной информацией по аналогии действия “логической бомбы”.

При рассмотрении вопросов, касающихся программной защиты информационных ресурсов особо надо подчеркнуть проблему защиты их от компьютерных вирусов.

Здесь необходимо активно использовать специальные программные **антивирусные** средства защиты (как зарубежного, так и отечественного производства). Антивирусные программы своевременно обнаруживают, распознают вирус в информационных ресурсах, а также “лечат” их.

Однако, наряду с использованием антивирусных программ, для уменьшения опасности вирусных посягательств на СКТ необходимо предпринять **комплексные организационно-технические меры.**

1. Информировать всех сотрудников учреждения, организации, использующих СКТ, об опасности и возможном ущербе в случае совершения вирусного посягательства.

2. Запретить сотрудникам приносить на рабочее место программные средства (ПС) “со стороны” для работы с ними на СКТ учреждения, организации по месту работы сотрудника.

3. Запретить сотрудникам использовать, хранить на носителях и в памяти ЭВМ компьютерные игры.

4. Предостеречь сотрудников организации от использования ПС и носителей машинной информации, имеющих происхождение из учебных заведений различного уровня и профиля.

5. Все файлы, которые поступают из внешней компьютерной сети должны обязательно тестироваться.

6. Создать архив копий ПС, используемых в непосредственной работе организации.

7. Регулярно просматривать хранимые в компьютерной системе ПС, создавать новые их архивные копии; где это возможно, использовать защиту типа “только чтение” для предупреждения несанкционированных манипуляций с ценными данными.

8. Периодически проводить ревизионную проверку контрольных сумм файлов, путем их сличения с эталоном.

9. Использовать для нужд электронной почты отдельный стендовый компьютер или ввести специальный отчет.

10. Установить системы защиты информации на особо важных ЭВМ. Заактивировать на них специальные комплексные антивирусные ПС.

11. Постоянно контролировать исполнение установленных правил обеспечения безопасности СКТ и применять меры дисциплинарного воздействия к лицам, сознательно или неоднократно нарушавшим их и т.д.

Компьютерные вирусы, их классификация и поражающие особенности

Компьютерный вирус — это специальная программа, способная самопроизвольно присоединяться к другим программам и при запуске последних выполнять различные нежелательные действия: порчу файлов и каталогов; искажение результатов вычислений; засорение или стирание памяти; создание помех в работе компьютера. Наличие вирусов проявляется в разных ситуациях.

- Некоторые программы перестают работать или начинают работать некорректно.
- На экран выводятся посторонние сообщения, сигналы и другие эффекты.
- Работа компьютера существенно замедляется.
- Структура некоторых файлов оказывается испорченной.

Имеются несколько признаков классификации существующих вирусов:

- по среде обитания;
- по области поражения;
- по особенности алгоритма;
- по способу заражения;
- по деструктивным возможностям.

По среде обитания различают ***файловые***, ***загрузочные***, ***макро- и сетевые вирусы***.

Файловые вирусы — наиболее распространенный тип вирусов. Эти вирусы внедряются в выполняемые файлы, создают файлы-спутники (companion-вирусы) или используют особенности организации файловой системы (link-вирусы).

Загрузочные вирусы записывают себя в загрузочный сектор диска или в сектор системного загрузчика жесткого диска. Начинают работу при загрузке компьютера и обычно становятся резидентными.

Макровирусы заражают файлы широко используемых пакетов обработки данных. Эти вирусы представляют собой программы, написанные на встроенных в эти пакеты языках программирования. Наибольшее распространение получили макровирусы для приложений Microsoft Office.

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. Полноценные компьютерные вирусы при этом обладают возможностью запустить на удаленном компьютере свой код на выполнение.

На практике существуют разнообразные сочетания вирусов — например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные секторы дисков, или сетевые макровирусы, которые заражают редактируемые документы и рассылают свои копии по электронной почте.

Как правило, каждый вирус заражает файлы одной или нескольких ОС. Многие загрузочные вирусы также ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков. По особенностям алгоритма выделяют резидентные вирусы, стелс-вирусы, полиморфные и др.

Резидентные вирусы способны оставлять свои копии в ОП, перехватывать обработку событий (например, обращение к файлам или дискам) и вызывать при этом процедуры заражения объектов (файлов или секторов).

Стелс-вирусы при этом либо временно лечат эти объекты, либо подставляют вместо себя незараженные участки информации. Частично к стелс-вирусам относят небольшую группу макровирусов, хранящих свой основной код не в макросах, а в других областях документа — в его переменных или в Auto-text.

Полиморфность (самошифрование) используется для усложнения процедуры обнаружения вируса. Полиморфные вирусы — это трудно выявляемые вирусы, не имеющие постоянного участка кода. В общем случае два образца одного и того же вируса не имеют совпадений. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

При создании вирусов часто используются нестандартные приемы. Их применение должно максимально затруднить обнаружение и удаление вируса.

Эти вирусы активны в памяти не только в момент работы зараженной программы, но и после. Резидентные копии таких вирусов жизнеспособны до перезагрузки ОС, даже если на диске уничтожены все зараженные файлы. Если резидентный вирус является также загрузочным и активизируется при загрузке ОС, то даже форматирование диска при наличии в памяти этого вируса его не удаляет.

К разновидности резидентных вирусов следует отнести также макровирусы, поскольку они постоянно присутствуют в памяти компьютера во время работы зараженного редактора.

Стелс-алгоритмы позволяют вирусам полностью или частично скрыть свое присутствие. Наиболее распространенным стелс-алгоритмом является перехват запросов ОС на чтение/запись зараженных объектов.

При инсталляции эти утилиты самостоятельно устанавливают на компьютере систему скрытого удаленного управления. В результате возникает возможность скрытого управления этим компьютером. Реализуя заложенные алгоритмы, утилиты без ведома пользователя принимают, запускают или отсылают файлы, уничтожают информацию, перезагружают компьютер и т. д. Возможно использование этих утилит для обнаружения и передачи паролей и ной конфиденциальной информации, запуска вирусов, уничтожения данных.

К Intended-вирусам относятся программы, которые не способны размножаться из-за существующих в них ошибок. К этому классу также можно отнести вирусы, которые размножаются только один раз. Заразив какой-либо файл, они теряют способность к дальнейшему размножению через него.

По способу заражения различают троянские программы, утилиты скрытого администрирования, Intended-вирусы и т. д.

Троянские программы получили свое название по аналогии с троянским конем. Назначение этих программ — имитация каких-либо полезных программ, новых версий популярных утилит или дополнений к ним. При их записи пользователем на свой компьютер троянские программы активизируются и выполняют нежелательные действия.

Разновидностью троянских программ являются утилиты скрытого администрирования. По своей функциональности и интерфейсу они во многом напоминают системы администрирования компьютеров в сети, разрабатываемые и распространяемые различными фирмами — производителями программных продуктов.

По деструктивным возможностям вирусы разделяются на:

- неопасные, влияние которых ограничивается уменьшением свободной памяти на диске, замедлением работы компьютера, графическим и звуковыми эффектами;
- опасные, которые потенциально могут привести к нарушениям в структуре файлов и сбоям в работе компьютера;
- очень опасные, в алгоритм которых специально заложены процедуры уничтожения данных и возможность обеспечивать быстрый износ движущихся частей механизмов путем ввода в резонанс и разрушения головок чтения/записи некоторых НЖМД (накопителей на жестких магнитных дисках).

Для борьбы с вирусами существуют программы, которые можно разбить на основные группы: мониторы, детекторы, доктора, ревизоры и вакцины.

Программы-мониторы (программы-фильтры) располагаются резидентно в ОП компьютера, перехватывают и сообщают пользователю об обращениях ОС, которые используются вирусами для размножения и нанесения ущерба. Пользователь имеет возможность разрешить или запретить выполнение этих обращений. К преимуществу таких программ относится возможность обнаружения неизвестных вирусов. Использование программ-фильтров позволяет обнаруживать вирусы на ранней стадии заражения компьютера. Недостатками программ являются невозможность отслеживания вирусов, обращающихся непосредственно к BIOS, а также загрузочных вирусов, активизирующихся до запуска антивируса при загрузке DOS, и частая выдача запросов на выполнение операций.

Программы-детекторы проверяют, имеется ли в файлах и на дисках специфическая для данного вируса комбинация байтов. При ее обнаружении выводится соответствующее сообщение. Недостаток — возможность защиты только от известных вирусов.

Программы-доктора восстанавливают зараженные программы путем удаления из них тела вируса. Обычно эти программы рассчитаны на конкретные типы вирусов и основаны на сравнении последовательности кодов, содержащихся в теле вируса, с кодами проверяемых программ. Программы-доктора необходимо периодически обновлять с целью получения новых версий, обнаруживающих новые виды вирусов.

Программы-ревизоры анализируют изменения состояния файлов и системных областей диска. Проверяют состояние загрузочного сектора и таблицы FAT; длину, атрибуты и время создания файлов; контрольную сумму кодов. Пользователю сообщается о выявлении несоответствий.

Программы-вакцины модифицируют программы и риски так, что это не отражается на работе программ, но вирус, от которого производится вакцинация, считает программы или диски уже зараженными. Существующие антивирусные программы в основном относятся к классу гибридных (детекторы-доктора, доктора-ревизоры и пр.).

В России наибольшее распространение получили антивирусные программы Лаборатории Касперского (Anti-IViral Toolkit Pro) и ДиалогНаука (Adinf,Dr.Web). Антивирусный пакет AntiViral Toolkit Pro (AVP) включает AVP Сканер, резидентный сторож AVP Монитор, программу администрирования установленных компонентов. Центр управления и ряд других. AVP Сканер помимо традиционной проверки выполняемых файлов и файлов документов обрабатывает базы данных электронной почты. Использование сканера позволяет выявить вирусы в упакованных и архивированных файлах (не защищенных паролями). Обнаруживает к удаляет макровирусы, полиморфные, стелс, троянские, а также ранее неизвестные вирусы. Это достигается, например, за счет использования эвристических анализаторов.

Методы защиты информации при использовании компьютерных сетей

На сегодняшний день сформулировано три базовых принципа информационной безопасности, которая должна обеспечивать.

- целостность данных - защиту от сбоев, ведущих к потере информации, а также неавторизованного создания или уничтожения данных;
- конфиденциальность информации и, одновременно,
- ее доступность для всех авторизованных пользователей.

Следует также отметить, что отдельные сферы деятельности (банковские и финансовые институты, информационные сети, системы государственного управления, оборонные и специальные структуры) требуют специальных мер безопасности данных и предъявляют повышенные требования к надежности функционирования информационных систем, в соответствии с характером и важностью решаемых ими задач.

При рассмотрении проблем защиты данных в сети прежде всего возникает вопрос о классификации сбоев и нарушений прав доступа, которые могут привести к уничтожению или нежелательной модификации данных.

Среди таких потенциальных "угроз" можно выделить:

1. Сбои оборудования:

- сбои кабельной системы;
- перебои электропитания;
- сбои дисковых систем;
- сбои систем архивации данных;
- сбои работы серверов, рабочих станций, сетевых карт и т. д.;

2. Потери информации из-за некорректной работы ПО:

- потеря или изменение данных при ошибках ПО;
- потери при заражении системы компьютерными вирусами;

3. Потери, связанные с несанкционированным доступом:

- несанкционированное копирование, уничтожение или подделка информации;
- ознакомление с конфиденциальной информацией, составляющей тайну, посторонних лиц;

4. Потери информации, связанные с неправильным хранением архивных данных.

5. Ошибки обслуживающего персонала и пользователей.

- случайное уничтожение или изменение данных;

- некорректное использование программного и аппаратного обеспечения, ведущее к уничтожению или изменению данных.

В зависимости от возможных видов нарушений работы сети (в том числе и несанкционированный доступ) многочисленные виды защиты информации объединяются в три основных класса:

- средства физической защиты, включающие средства защиты кабельной системы, систем электропитания, средства архивации, дисковые массивы и т. д.

- программные средства защиты, в том числе: антивирусные программы, системы разграничения полномочий, программные средства контроля доступа.
- административные меры защиты, включающие контроль доступа в помещения, разработку стратегии безопасности фирмы, планов действий в чрезвычайных ситуациях и т.д.

Метод «интеллектуального перебора паролей»

Метод «интеллектуального перебора» основан на подборе предполагаемого пароля, исходя из заранее определенных тематических групп его принадлежности. Интересны результаты экспериментов, представленные специалистами в форме таблицы:

№	Тематические группы паролей	% частоты выбора пароля человеком	% раскрываемости пароля
1	Имена, фамилии и производные	22,2	54,5
2	Интересы (хобби, спорт, музыка)	9,5	29,2
3	Даты рождения, знаки зодиака свои и близких; их комбинация с 1-ой группой	11,8	54,5
4	Адрес жительства, место рождения	4,7	55,0
5	Номера телефонов	3,5	66,6
6	Последовательность клавиш ПК, повтор символа	16,1	72,3
7	Номера документов (паспорт, пропуск, удостоверение и т.д.)	3,5	100,0
8	Прочие	30,7	5,7

Данная статистика раскрываемости паролей должна стать предостережением «любителям» установки тематических паролей – они являются ненадежными, так как очень легко раскрываются.

При составлении паролей рекомендуется придерживаться следующих правил:

- Пароль должен содержать не менее **шести** символов.
- В состав пароля могут входить цифры, латинские буквы, пробелы и специальные символы («**.**», «**,**», «**?**», «**!**», «**<**», «**>**». «**”**» и др.).
- Рекомендуется составлять пароль из смешанного набора цифровых и буквенных (прописных и строчных) символов.

Не используйте в качестве пароля:

Общеупотребительные слова и устойчивые словосочетания.

Наборы символов, представляющие собой комбинации клавиш, расположенных подряд на клавиатуре, такие как: **qwerty**, **123456789**, **qazxsw** и т. п.

Персональные данные: **имена** и **фамилии**, **адреса**, **номера паспортов**, **страховых свидетельств** и т. п., пароли, созданные для доступа к другим программам (электронная почта, базы данных и пр.).

Пример алгоритма создания паролей №1

Вы можете создавать свои алгоритмы генерации паролей:

Сделайте начало (середину или конец) всех паролей одинаковым, например, **l8H!p1n**.

К нему добавьте части, которые ассоциируются с конкретным сервисом, для которого этот пароль предназначен, например, для почты — **mail**. В результате получим **l8H!p1nmail**.

Однако при хищении паролей злоумышленником алгоритм может быть легко определен. Поэтому для регистрации на подозрительных сервисах используйте любую другую отвлеченную комбинацию символов.

Пример алгоритма создания паролей №2

Петров Иван Сергеевич 18 апреля 1982 года рождения для регистрации на сайте **superpochta.ru** может задать следующую последовательность:

Последние четыре символа адреса прописными буквами (**superpochta.ru** = **A.RU**).

Сумма даты и месяца рождения с количеством согласных букв в адресе сайта (**18+4+7=29**).

Предпоследние три буквы отчества, набранные транслитом (**Сергеевич** = **evi**).

В результате получается пароль **A.RU29evi**.

Используя подобные алгоритмы, можно генерировать огромное количество сложных паролей.

Правовое обеспечение информационной безопасности

Современный этап развития системы обеспечения информационной безопасности государства и общества характеризуется переходом от тотального сокрытия большого объема сведений к гарантированной защищенности принципиально важных данных, обеспечивающей:

- конституционные права и свободы граждан, предприятий и организаций в сфере информатизации;
- необходимый уровень безопасности информации, подлежащей защите;
- защищенность систем формирования и использования информационных ресурсов (технологий, систем обработки и передачи

Ключевым моментом политики государства в данной области является осознание необходимости защиты любых информационных ресурсов и информационных технологий, неправомерное обращение с которыми может нанести ущерб их собственнику, владельцу, пользователю или иному лицу.

Нормативные акты правового регулирования вопросов информатизации и защиты информации в Российской Федерации включают:

- Законы Российской Федерации
- Указы Президента Российской Федерации и утверждаемые этими указами нормативные документы
- Постановления Правительства Российской Федерации и утверждаемые этими постановлениями нормативные документы

- Государственные и отраслевые стандарты
- Положения, Порядки. Руководящие документы и другие нормативные и методические документы уполномоченных государственных органов (Гостехкомиссии России, ФАПСИ, ФСБ).

Федеральные законы и другие нормативные акты предусматривают:

- разделение информации на категории свободного и ограниченного доступа, причем информация ограниченного доступа подразделяется на:
  - отнесенную к государственной тайне
  - отнесенную к служебной тайне (информацию для служебного пользования), персональные данные (и другие виды тайн)
  - и другую информацию, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю или иному лицу;

- *правовой режим защиты информации*, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу, устанавливаемый:
- в отношении сведений, отнесенных к государственной тайне, -уполномоченными государственными органами на основании Закона Российской Федерации "О государственной тайне" (от 21.07.93 г. N 5485-1);
- в отношении конфиденциальной документированной информации -собственником информационных ресурсов или уполномоченным лицом на основании Закона Российской Федерации "Об информации, информатизации и защите информации" (от 20.02.95 г. N 24-ФЗ);
- в отношении персональных данных - отдельным федеральным законом;

- *лицензирование деятельности* предприятий, учреждений и организаций в области защиты информации;
- *аттестование* автоматизированных информационных систем, обрабатывающих информацию с ограниченным доступом на соответствие требованиям безопасности информации при проведении работ со сведениями соответствующей степени конфиденциальности (секретности);
- *сертификацию средств защиты* информации и средств контроля эффективности защиты, используемых в АС;
- возложение решения вопросов организации лицензирования, аттестации и сертификации на органы государственного управления в пределах их компетенции, определенной законодательством Российской Федерации;

- создание автоматизированных информационных систем в защищенном исполнении и специальных подразделений, обеспечивающих защиту информации с ограниченным доступом, являющейся собственностью государства, а также осуществление контроля защищенности информации и предоставление прав запрещать или приостанавливать обработку информации в случае невыполнения требований по обеспечению ее защиты;
- определение прав и обязанностей субъектов в области защиты информации.

Конец