Защита от несанкционированного доступа к информации

Храмцова Елена Николаевна,
учитель информатики
МАОУ «СОШ №94»

Несанкционированный доступ (НСД) злоумышленника на компьютер опасен не только возможностью прочтения и/или модификации обрабатываемых электронных документов, но и возможностью внедрения злоумышленником управляемой программной закладки, которая позволит ему предпринимать следующие действия:

- Читать и/или модифицировать электронные документы, которые в дальнейшем будут храниться или редактироваться на компьютере.
- Осуществлять перехват различной ключевой информации, используемой для защиты электронных документов.
- Использовать захваченный компьютер в качестве плацдарма для захвата других компьютеров локальной сети.
- Уничтожить хранящуюся на компьютере информацию или вывести компьютер из строя путем запуска вредоносного программного обеспечения.

Специалист по защите информации

То, что придумывают одни, всегда пытаются использовать другие.

И первые рано или поздно начинают защищать плоды собственного интеллекта.

Так появилась **одна из наиболее ценных и востребованных на сегодняшний день профессий - специалист по защите информации.**

Сегодня, разумеется, неразрывно связанная с компьютерами.

Вначале система информационной безопасности разрабатывались **для нужд военных.**

Стратегические данные, касающиеся обороноспособности, были настолько важны, что их утечка могла привести к огромным людским потерям.

Соответственно, **компьютерная безопасность обратилась к опыту криптографии, то есть шифрования.**

Появлялись криптошрифты и специальные **программы**, позволяющие автоматизировать процесс шифровки и дешифровки.

Позже, когда необходимость защиты информации распространилась на иные сферы, стало понятно, что иногда **шифрование сильно затрудняет и замедляет передачу и использование данных.** А с развитием компьютерных сетей и систем стали появляться другие задачи.

Со временем появилась классификация тайн, которые необходимо защищать.

Они составили шесть категорий: **государственная тайна, коммерческая, банковская, профессиональная, служебная и персональные данные.**

Понятно, что для разных отраслей и типов предприятий приоритетными оказываются одна или две категории. Производству, связанному с наукой, например, крайне важно предотвратить утечку планов, новых разработок и испытаний.

Специалисты считают, что сегодня, в отличие от прошлых десятилетий, больше внимания уделяется двум вещам: доступности и целостности информации.

Доступность означает тот факт, что каждый пользователь может в любое время затребовать необходимый сервис и работать в нем без осложнений.

С другой стороны - во время хранения и передачи информация должна оставаться **целостной**.

Особенно актуально это, например, для банков, где важно не допустить изменения реквизитов, приписывания лишних ноликов.

В то же время, **провайдерам или операторам связи** абсолютно необходимо сохранять доступность и безотказность работы информационных систем (сервера, узла связи), потому что именно это является основой успеха.

От кого защищать?

Итак, современная защита информации - это поиск оптимального соотношения между доступностью и безопасностью.

Или, другими словами, это постоянная борьба с **глупостью пользователей и интеллектом хакеров.**

Существует несколько мифов о том, кто больше всего покушается на чужую информацию.

Например, несколько **преувеличивают шансы нападения хакеров**. Это, мол, такие проворные ребята, которые только и делают, что воруют деньги с банковских счетов и разрушают национальные системы безопасности. От них и стоит всячески защищаться.

На самом деле хакеры берут не числом, а умением.

А статистика говорит, что 70-80% компьютерных преступлений совершаются работающими или уволенными сотрудниками, то есть **внутри компаний**.

Иногда люди, обладающие большими полномочиями, паролями и доступом к информации, не могут одолеть соблазна воспользоваться этими преимуществами.

А те, кого уволили, таким образом мстят фирме, отделу или лично уволившему начальнику.

Что же касается хакеров, то сегодня многие из них совершенно легально занимаются тестированием новых программ защиты.

Собственно, тестирование заключается в том, что программу пытаются взломать и наблюдают за ее "реакцией".

Именно это рождает на Западе самые серьезные сложности во взаимоотношениях с государством.

Дело в том, что в 1998 году в США был принят один из самых спорных законов - DCMA (Digital Millennium Copyright Act) - "Акт об авторских правах в цифровой век".

Он **запретил обходить защиту** от копирования и распространять устройства, которые можно использовать для нарушения авторских прав.

Причем наказание по этому закону следует даже в том случае, когда взломщик не сделал ничего, кроме самого взлома, не причинил материального ущерба.

После того как специалист проверяет надежность защиты программного обеспечения и публикует информацию о ее слабых местах, его могут привлечь к ответственности за нарушение закона.

Доказательством серьезности проблемы стали уголовное преследование профессора ВТ Принстонского университета **Эдварда Фелтена** и арест российского специалиста по шифрованию **Дмитрия Склярова**.

Многие программисты, занимающиеся компьютерной безопасностью, вынуждены "уйти в тень.

Ну а главные сторонники и защитники закона, разумеется, производители ПО, **Голливуд и музыкальная индустрия**.

Существует притча о самом надежном способе хранения информации:

Информация должна быть в одном экземпляре на компьютере, который находится в бронированном сейфе, отключенный **от всех сетей и обесточенный.**

Понятно, что работать с такой информацией, мягко говоря, неудобно.

В то же время хочется защитить программы и данные от несанкционированного доступа (НСД).

А чтобы доступ был санкционированным, нужно определиться, кому что можно, а что нельзя.

Цели злоумышленников:

- **использование компьютера** для взлома других компьютеров, атак на сайты, рассылки спама, подбора паролей
- **кража** секретной информации — данных о банковских картах, паролей
- **мошенничество** (хищение путём обмана)
  - «нигерийские» письма (хищение денег)
  - «фишинг» (выманивание паролей через подставные сайты)
  - блокировка с требованием SMS

Воры пользуются программам типа "троянский конь"

(устанавливаются на компьютер, самые простые просто крадут все пароли, продвинутые - позволяют просматривать содержимое экрана, перехватывать все вводимые с клавиатуры клавиши, изменять файлы и т.д.).

Модными стали также атаки под названием "отказ в обслуживании", которые выводят из строя узлы сети.

При этом работа узла становится невозможной на протяжении нескольких минут или даже часов.

Понятно, что подобные остановки приносят огромные убытки.

Виды защиты информации

- средства физической защиты
- программные средства(антивирусные средства, системы разграничения полномочий)
- административные меры защиты(доступ в помещение, разработка стратегий безопасности)

Средства физической защиты

Системы защиты информации обеспечивают выполнение **следующих функций:**

- идентификация,
- аутентификация, т.е. установление подлинности на основе сравнения с эталонными идентификаторами;
- разграничение доступа пользователей;
- регистрация событий:
  - входа пользователя в систему,
  - выхода пользователя из системы,
  - нарушения прав доступа;

Основные достоинства **биометрических** методов идентификации и аутентификации:

- высокая степень достоверности идентификации по биометрических признакам из-за их уникальности;
- неотделимость биометрических признаков от дееспособной личности;
- трудность фальсификации биометрических признаков.

В качестве **биометрических признаков**, которые могут быть использованы для идентификации потенциального пользователя, используются:

- узор радужной оболочки и сетчатки глаз;
- отпечатки пальцев;
- геометрическая форма руки;
- форма и размеры лица;
- форма ушей;
- особенности голоса;
- ДНК;
- биомеханические характеристики рукописной подписи;
- и др.

Идентификация по отпечаткам пальцев

Оптические сканеры считывания отпечатков пальцев устанавливаются на ноутбуки, мыши, клавиатуры, флэш-диски, а

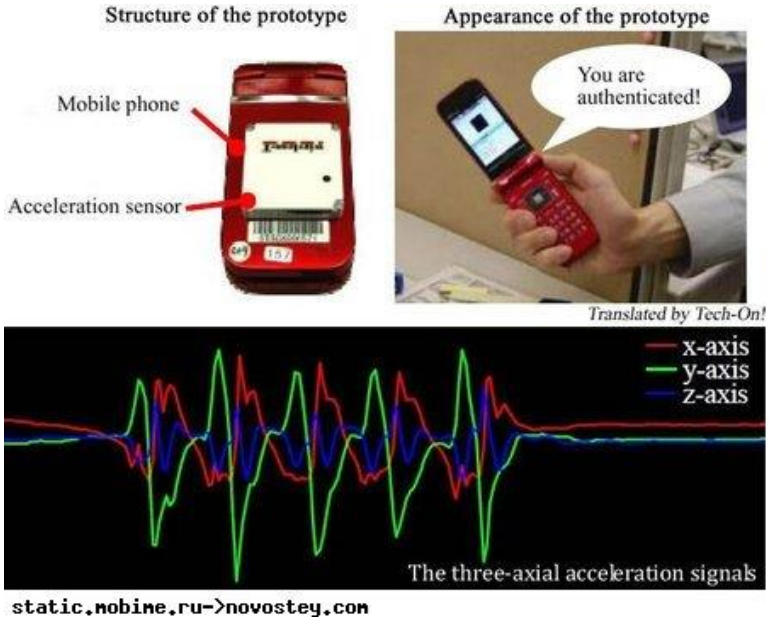
также применяются в виде **отдельных внешних устройств и терминалов** (например, в аэропортах и банках).

. Оптический сканер отпечатка пальца, вмонтированный в ноутбук

Идентификация человека по голосу — один из традиционных способов распознавания

Интерес к этому методу связан и с прогнозами внедрения голосовых интерфейсов в операционные системы.

Голосовая идентификация бесконтактна и существуют системы ограничения доступа к информации на основании частотного анализа речи.



Идентификация по радужной оболочке глаза

Радужная оболочка глаза является уникальной для каждого человека биометрической характеристикой.

Изображение глаза выделяется из изображения лица и на него накладывается специальная маска штрих-кодов. Результатом является матрица, индивидуальная для каждого человека.

Идентификация по изображению лица

Для идентификации личности часто используются технологии распознавания по лицу. Распознавание человека происходит на расстоянии.

Идентификационные признаки учитывают форму лица, его цвет, а также цвет волос. К важным признакам можно отнести также **координаты точек лица** в местах, соответствующих смене контраста (брови, глаза, нос, уши, рот и овал).

В настоящее время начинается выдача новых загранпаспортов, в микросхеме которых хранится цифровая фотография владельца.

Идентификация по ладони руки

В биометрике в целях идентификации используется простая геометрия руки — размеры и форма, а также некоторые информационные знаки на тыльной стороне руки (образы на сгибах между фалангами пальцев, узоры расположения кровеносных сосудов).

Сканеры идентификации по ладони руки установлены в некоторых аэропортах, банках и на атомных электростанциях

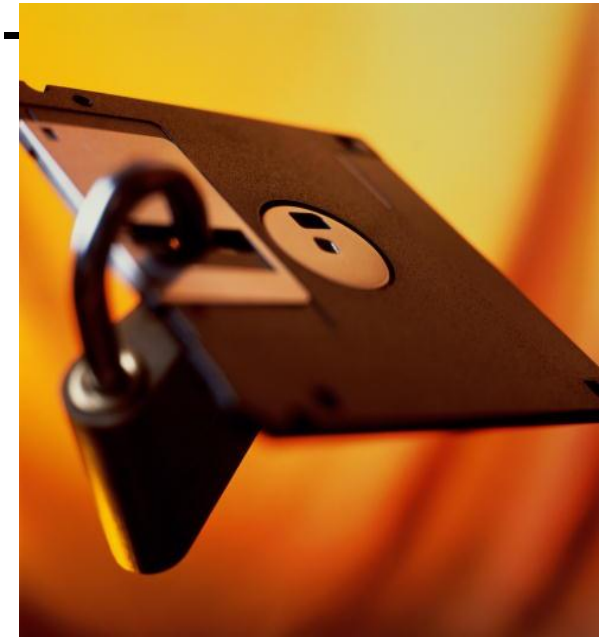
Программные средства защиты

Защита от несанкционированного копирования включает:

- защиту сообщений от авторских правах разработчика, выводимой программой на экран или находящихся внутри программы
- защиту от модификаций программы
- собственно защиту от незаконного тиражирования программы тем или иным способом.

Виды защиты информации от копирования

- Защита с помощью серийного номера
- Использование технических отличий в машине для программной защиты
- Использование программно-аппаратной защиты



Информационная безопасность — это состояние защищённости информационной среды.

- надежность работы компьютера,
- сохранность ценных данных,
- защиту информации от внесения в нее изменений неуполномоченными лицами,
- сохранение тайны переписки в электронной связи.

Принципы работы специалиста по защите информации

Все меньше он занимается физической безопасностью (пропускным режимом, видеонаблюдением и т.д.) и все больше - сетевой и компьютерной.

Существует принципиальная схема, по которой строится работа такого специалиста.

Во-первых, он проводит информационное обследование и анализ

Это самый важный этап, в результате которого появляется так называемая "модель нарушителя": кто, зачем и как может нарушать безопасность. Чтобы грамотно провести обследование, профессионал должен знать основные направления **экономического и социального развития отрасли**, перспективы, специализацию и особенности предприятия, специфику работы конкурентов, детали прохождения информации по подразделениям, знать кадровые проблемы и быть в курсе "подводных течений" в коллективе.

На ***втором этапе*** разрабатываются внутренние организационно-правовые документы, которые максимально упорядочивают информационные потоки.

Понятно, что здесь необходимы дополнительные знания: законодательства и права, основ организации, планирования и управления предприятием, делопроизводства и т.п.

Далее специалист по защите информации руководит приобретением, установкой и настройкой средств и механизмов защиты.

И здесь ему не обойтись без серьезной подготовки:

информационные технологии и программирование, квантовая и оптическая электроника, радиоэлектроника, криптографические методы защиты, безопасность жизнедеятельности.

И, наконец, на следующем этапе необходимо поддерживать, обновлять, модернизировать созданную систему безопасности.

Крупнейшие банки, например, меняют программное обеспечение, отвечающее за защиту, примерно раз в полгода.

В отделах, которые занимаются безопасностью, работают, как правило, наиболее опытные программисты,

которые постоянно проходят обучение и получают дополнительную квалификацию.

Из наиболее серьезных учебных заведений **Москвы,** выпускники которых пользуются спросом на этом рынке, можно перечислить шесть-семь.

- Первенство и по качеству, и по накопленному опыту, и по технической оснащенности держит, понятное дело, Академия федеральной службы безопасности РФ, в структуре которой есть отдельный институт, готовящий специалистов данного профиля.

Далее следуют Национальный исследовательский ядерный университет «МИФИ» (факультет информационной безопасности),

Московский государственный технический университет имени Н.Э. Баумана (факультет информатики и систем управления),

Российский государственный гуманитарный университет (факультет защиты информации),

Московский государственный институт радиотехники, электроники и автоматики (факультет вычислительных машин и систем),

Московский государственный институт электроники и математики (факультет прикладной математики),
Московский государственный институт электронной техники (факультет микроприборов и технической кибернетики).

Специалистов в области защиты информации готовят в учебных заведениях г. Томска и Новосибирска.

По прогнозам специалистов, **значимость специалистов по защите информации будет расти.** Мы постепенно приближаемся к западной модели управления - там руководители подобных отделов входят в совет директоров и часто становятся вторым-третьим лицом в компании. Кроме того, появляется спрос на создание **национальных систем компьютерной безопасности**, а вслед за этим и приглашение специалистов на государственные должности.

Эти люди иногда становятся весьма важными политическими персонами (как, например,

Ричард Кларк,

член Национального совета по безопасности, советник президента США по компьютерной безопасности, отвечающий за защиту национальных коммуникаций и информационных инфраструктур от террористических актов в "сети").

Стать квалифицированным, высоко оплачиваемым специалистом по защите информации может человек, обладающий природной, врожденной психологической стабильностью.

Об этом говорят не только психологи, но и эксперты.

Умение хранить чужие тайны - это тоже талант, который невозможно заменить набором знаний.

Федеральный закон «Об информации и защите информации»

- Закон РФ «Об авторском праве и смежных правах»
- ©

Правила личной безопасности

- не работать с правами **администратора**
- не запоминать **пароли** в браузере
- использовать флажок «**Чужой компьютер**»
- не использовать стандартные **секретные вопросы** (любимое блюдо, кличка собаки, девичья фамилия матери и т.п.)
- не размещать информацию, которая может **повредить**
- **шифровать** данные (архив с паролем)
- денежные операции – по протоколу **HTTPS** *(Hypertext Transfer Protocol **Secure**)*

Источники

1. Журнал «Обучение в России»
2. «Методы и средства защиты от несанкционированного доступа», © *Панасенко Сергей, 2005*. Ссылка
3. Поляков К.Ю., Еремин Е.А. Презентация по информационной безопасности сайт