Защита информационных ресурсов от несанкционированного доступа

Выполнила: Рябова Полина
311 фарм Б

Использование компьютеров и автоматизированных технологий приводит к появлению ряда проблем для руководства организацией. Компьютеры, часто объединенные в сети, могут предоставлять доступ к колоссальному количеству самых разнообразных данных. Поэтому люди беспокоятся о безопасности информации и наличии рисков, связанных с автоматизацией и предоставлением гораздо большего доступа к конфиденциальным, персональным или другим критическим данным. Электронные средства хранения даже более уязвимы, чем бумажные: размещаемые на них данные можно и уничтожить, и скопировать, и незаметно видоизменить.

Признаки компьютерных преступлений:

· неавторизованное использование компьютерного времени;

· неавторизованные попытки доступа к файлам данных;

· кражи частей компьютеров;

· кражи программ;

· физическое разрушение оборудования;

· уничтожение данных или программ;

· неавторизованное владение дискетами, лентами или распечатками.

Это только самые очевидные признаки, на которые следует обратить внимание при выявлении компьютерных преступлений. Иногда эти признаки говорят о том, что преступление уже совершено, или что не выполняются меры защиты. Они также могут свидетельствовать о наличии уязвимых мест и указать, где находится брешь в защите. В то время как признаки могут помочь выявить преступление или злоупотребление, меры защиты могут помочь предотвратить его.

Защита информации – это деятельность по предотвращению утраты и утечки защищаемой информации.

Информационной безопасностью называют меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе. Информационная безопасность включает в себя меры по защите процессов создания данных, их ввода, обработки и вывода.

Принципы защиты информации :

ПРИНЦИП ОБОСНОВАННОСТИ ДОСТУПА. Данный принцип заключается в обязательном выполнении двух основных условий: пользователь должен иметь достаточную «форму допуска» для получения информации требуемого им уровня конфиденциальности, и эта информация необходима ему для выполнения его производственных функций.

ПРИНЦИП ДОСТАТОЧНОЙ ГЛУБИНЫ КОНТРОЛЯ ДОСТУПА. Средства защиты информации должны включать механизмы контроля доступа ко всем видам информационных и программных ресурсов системы, которые с принципом обоснованности доступа следует разделять между пользователями.

ПРИНЦИП РАЗГРАНИЧЕНИЯ ПОТОКОВ ИНФОРМАЦИИ. Для предупреждения нарушения безопасности информации, которое, например, может иметь место при записи секретной информации на несекретные носители и несекретные файлы, ее передаче программам и процессам, не предназначенным для обработки секретной информации, а также при передаче секретной информации по незащищенным каналам и линиям связи, необходимо осуществлять соответствующее разграничение потоков информации.

ПРИНЦИП ЧИСТОТЫ ПОВТОРНО ИСПОЛЬЗУЕМЫХ РЕСУРСОВ. Данный принцип заключается в очистке ресурсов, содержащих конфиденциальную информацию, при их удалении или освобождении пользователем до перераспределения этих ресурсов другим пользователям.

ПРИНЦИП ПЕРСОНАЛЬНОЙ ОТВЕТСТВЕННОСТИ. Каждый пользователь должен нести персональную ответственность за свою деятельность в системе, включая любые операции с конфиденциальной информацией в системе и возможные нарушения ее защиты, т.е. какие-либо случайные или умышленные действия, которые приводят или могут привести к несанкционированному ознакомлению с конфиденциальной информацией, ее искажению или уничтожению, или делают такую информацию недоступной для ее законных пользователей.

ПРИНЦИП ЦЕЛОСТНОСТИ СРЕДСТВ ЗАЩИТЫ. Данный принцип подразумевает, что средства защиты информации в системе должны точно выполнять свои функции в соответствии с перечисленными принципами и быть изолированными от пользователей, а для своего сопровождения должны включать специальный защищенный интерфейс для средств контроля, сигнализации о попытках нарушения защиты информации и воздействия на процессы в системе.

Информационная безопасность дает гарантию того, что достигаются следующие **цели**:
· конфиденциальность критической информации;
· целостность информации и связанных с ней процессов (создания, ввода, обработки и вывода);
· доступность информации, когда она нужна;
· учет всех процессов, связанных с информацией.

Под **критическими данными** понимаются данные, которые требуют защиты из-за вероятности нанесения ущерба и его величины в том случае, если произойдет случайное или умышленное раскрытие, изменение, или разрушение данных. К критическим также относят данные, которые при неправильном использовании или раскрытии могут отрицательно воздействовать на способности организации решать свои задачи; персональные данные и другие данные, защита которых требуется указами Президента РФ, законами РФ и другими подзаконными документами.

Технические, организационные и программные средства обеспечения сохранности и защиты от несанкционированного доступа

Существует четыре уровня защиты компьютерных и информационных ресурсов:

Предотвращение предполагает, что только авторизованный персонал имеет доступ к защищаемой информации и технологии.

Обнаружение предполагает раннее раскрытие преступлений и злоупотреблений, даже если механизмы защиты были обойдены.

Ограничение уменьшает размер потерь, если преступление все-таки произошло, несмотря на меры по его предотвращению и обнаружению.

Восстановление обеспечивает эффективное воссоздание информации при наличии документированных и проверенных планов по восстановлению.

Меры защиты - это меры, вводимые руководством, для обеспечения безопасности информации. К мерам защиты относят разработку административных руководящих документов, установку аппаратных устройств или дополнительных программ, основной целью которых является предотвращение преступлений и злоупотреблений.

Формирование режима информационной безопасности - проблема комплексная. Меры по ее решению можно разделить на **четыре уровня**:

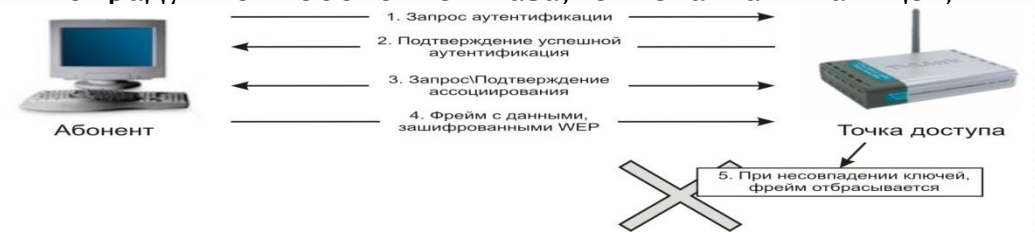
- **законодательный:** законы, нормативные акты, стандарты и т. п.;
-**административный:**действия общего характера, предпринимаемые руководством организации;
- **процедурный:** конкретные меры безопасности, имеющие дело с людьми;
- **программно-технический:** конкретные технические меры.

Рассмотрим некоторые меры защиты информационной безопасности компьютерных систем.

1. Аутентификация пользователей. Данная мера требует, чтобы пользователи выполняли процедуры входа в компьютер, используя это как средство для идентификации в начале работы. Для аутентификации личности каждого пользователя нужно использовать уникальные пароли, не являющиеся комбинациями личных данных пользователей, для пользователя. Необходимо внедрить меры защиты при администрировании паролей, и ознакомить пользователей с наиболее общими ошибками, позволяющими совершиться компьютерному преступлению. Если в компьютере имеется встроенный стандартный пароль, его нужно обязательно изменить.

Еще более надёжное решение состоит в организации контроля доступа в помещения или к конкретному компьютеру сети с помощью идентификационных пластиковых карточек с встроенной микросхемой - так называемых микропроцессорных карточек (smart - card). Их надёжность обусловлена в первую очередь невозможностью копирования или подделки кустарным способом. Установка специального считывающего устройства таких карточек возможна не только на входе в помещения, где расположены компьютеры, но и непосредственно на рабочих станциях и серверах сети.

Существуют также различные устройства для идентификации личности по биометрической информации - по радужной оболочке глаза, отпечаткам пальцев, размерам кисти руки и т.д.



2. Защита пароля.

Следующие правила полезны для защиты пароля:

· нельзя делится своим паролем ни с кем;

· пароль должен быть трудно угадываемым;

· для создания пароля нужно использовать строчные и прописные буквы, а еще лучше позволить компьютеру самому сгенерировать пароль;

· не рекомендуется использовать пароль, который является адресом, псевдонимом, именем родственника, телефонным номером или чем-либо очевидным;

· предпочтительно использовать длинные пароли, так как они более безопасны, лучше всего, чтобы пароль состоял из 6 и более символов;

· пароль не должен отображаться на экране компьютера при его вводе;

· пароли должны отсутствовать в распечатках;

· нельзя записывать пароли на столе, стене или терминале, его нужно держать в памяти;

· пароль нужно периодически менять и делать это не по графику;

· на должности администратора паролей должен быть самый надежный человек;

· не рекомендуется использовать один и тот же пароль для всех сотрудников в группе;

· когда сотрудник увольняется, необходимо сменить пароль;

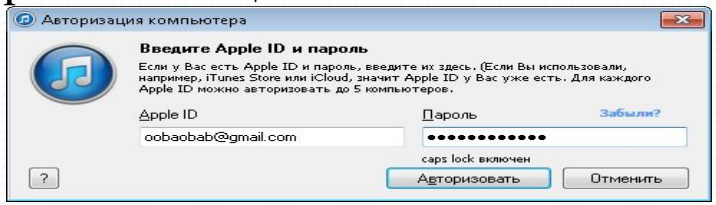
· сотрудники должны расписываться за получение паролей.

3. Процедуры авторизации.

В организации, имеющей дело с критическими данными, должны быть разработаны и внедрены процедуры авторизации, которые определяют, кто из пользователей должен иметь доступ к той или иной информации и приложениям.

В организации должен быть установлен такой порядок, при котором для использования компьютерных ресурсов, получения разрешения доступа к информации и приложениям, и получения пароля требуется разрешение тех или иных начальников.

Если информация обрабатывается на большом вычислительном центре, то необходимо контролировать физический доступ к вычислительной технике. Могут оказаться уместными такие методы, как журналы, замки и пропуска, а также охрана. Ответственный за информационную безопасность должен знать, кто имеет право доступа в помещения с компьютерным оборудованием и выгонять оттуда посторонних лиц.



4. Предосторожности при работе.

Рекомендуется:

· отключать неиспользуемые терминалы;

· закрывать комнаты, где находятся терминалы;

· разворачивать экраны компьютеров так, чтобы они не были видны со стороны двери, окон и прочих мест, которые не контролируются;

· установить специальное оборудование, ограничивающее число неудачных попыток доступа, или делающее обратный звонок для проверки личности пользователей, использующих телефоны для доступа к компьютеру

· использовать программы отключения терминала после определенного периода неиспользования;

· выключать систему в нерабочие часы;

· использовать системы, позволяющие после входа пользователя в систему сообщать ему время его последнего сеанса и число неудачных попыток установления сеанса после этого. Это позволит сделать пользователя составной частью системы проверки журналов.

Спасибо за внимание!!!