Организационные мероприятия администрирования. Понятие политики организации. Понятие режима доступа.

По методам применения тех или иных организационно технических мер предупреждения компьютерных преступлений специалистами отдельно выделяются основные группы:

1) организационные;

2) технические.

Организационные меры защиты ИС

Представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации аппаратуры телекоммуникаций для обеспечения защиты информации. Организационные мероприятия охватывают все структурные элементы аппаратуры на всех этапах их жизненного цикла (строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и эксплуатация)

Организационные меры защиты ИС 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 ИС;
- возложению дисциплинарной ответственности на лиц по обеспечению безопасности конкретных ИС;
- осуществлению режима секретности при функционировании компьютерных систем;
- обеспечению режима физической охраны объектов;
- материально-техническому обеспечению и т.д.

Причины и условия, способствующие совершению компьютерных преступлений

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;

3) ***низкий уровень программного обеспечения***;

4) ***несовершенство парольной системы защиты*** от несанкционированного доступа к рабочей станции и ее программному обеспечению;

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.

Организационные меры защиты ИС

Для эффективной безопасности от компьютерных преступлений всего лишь необходимо:

- просмотреть всю документацию в учреждении, организации;
- ознакомиться с функциями и степенью ответственности каждого сотрудника;
- определить возможные каналы утечки информации;
- ликвидировать обнаруженные слабые звенья в защите.

Организационные меры защиты ИС

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

1) для всех лиц, имеющих право доступа к ИС, 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 ИС (физическая охрана).

Технические меры защиты

Помимо организационно-управленческих мер, существенную общепрофилактическую роль в борьбе с компьютерными преступлениями могут играть также **меры технического характера**. Условно их можно подразделить на три основные группы в зависимости от характера и специфики охраняемого объекта, а именно:

- аппаратные;
- программные.

Технические меры защиты

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.

Аппаратные методы

Практическая реализация данных методов обычно осуществляется с помощью применения различных технических устройств специального назначения:

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

2) устройства экранирования аппаратуры, линий проводной связи и помещений;

3) устройства комплексной защиты телефонии;

4) устройства, обеспечивающие только санкционированный физический доступ пользователя на охраняемые объекты (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

Программные методы защиты предназначаются для непосредственной защиты информации по трем направлениям:

1) аппаратуры;

2) программного обеспечения;

3) данных и управляющих команд.

Программные методы

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).

Программные методы

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.***

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).

Программные методы

Антивирусные средства защиты - своевременно обнаруживают, распознают вирус в информационных ресурсах, а также “лечат” их.

- ***Сканеры*** - проверяют файлы, секторы дисков и системную память на наличие как известных, так и неизвестных типов вирусов.
- ***CRC-сканеры -*** подсчитывают контрольные суммы для вышеозначенных объектов.
- ***Мониторы*** - это резидентные программы, "перехватывающие" с их точки зрения подозрительные действия и сообщающие о них пользователю.
- ***Иммунизаторы*** делают систему невосприимчивой к тому или иному типу вирусов.