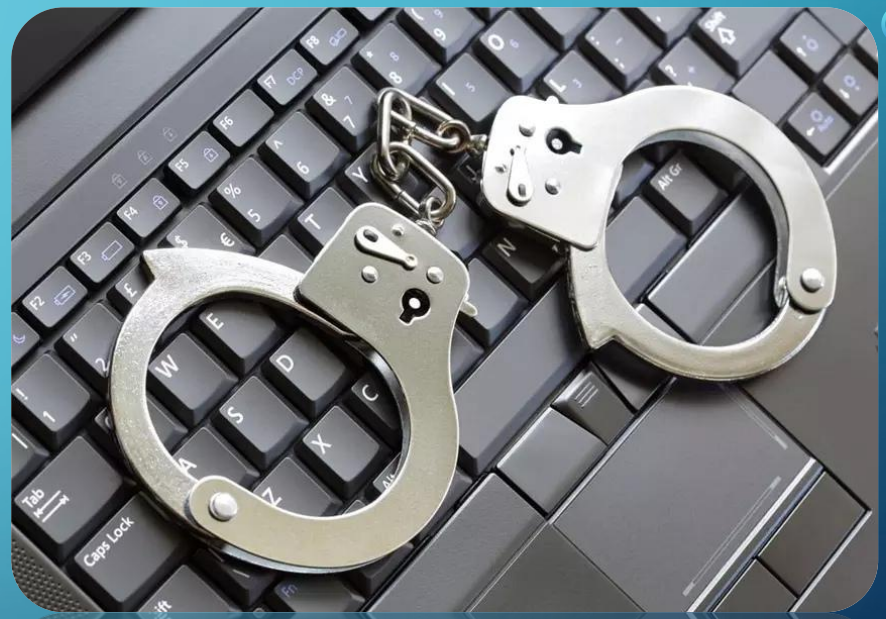
КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ

ОПРЕДЕЛЕНИЕ

Компьютерная преступность

(преступление с использованием компьютера) представляет собой любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку данных или передачу данных. При этом, компьютерная информация является предметом или средством совершения преступления. Структура и динамика компьютерной преступности в разных странах существенно отличается друг от друга. В юридическом понятии, компьютерных преступлений, как преступлений специфических не существует.

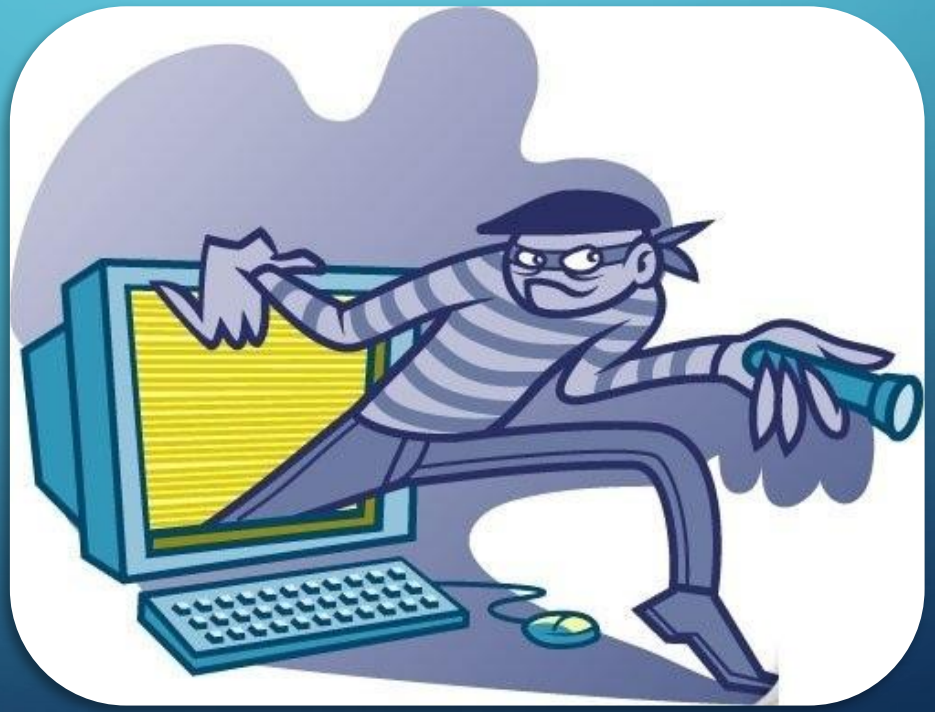


ВИДЫ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ:

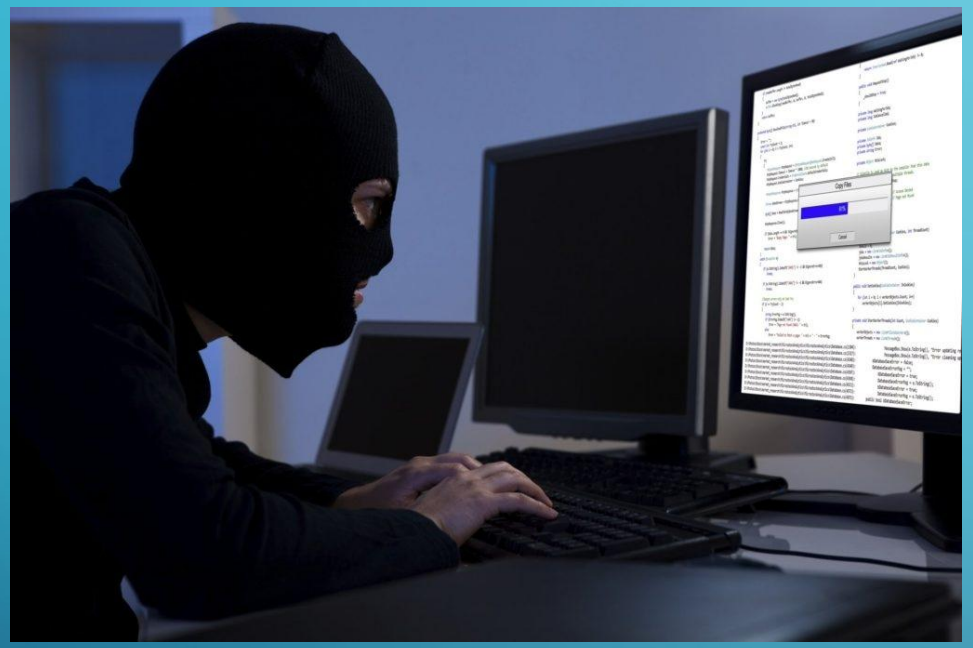
1. Внедрение компьютерного вируса
2. Несанкционированный доступ к информации
3. Подделка выходной информации
4. Несанкционированное копирование конфиденциальной информации

ВНЕДРЕНИЕ КОМПЬЮТЕРНОГО ВИРУСА-

-процесс внедрения вредоносной программы с целью нарушения работы ПК. Вирусы могут быть внедрены в операционную систему, прикладную программу или в сетевой драйвер. Вирус может проявлять себя в разных формах. Это могут быть замедления в выполнении программ; увеличение объёма программных файлов и наконец, эти проявления могут привести к стиранию файлов и уничтожению программного обеспечения.



НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К ИНФОРМАЦИИ-



- может осуществляться с целью её хищения или же ради развлечения и последующего использования данной информации. Существуют множество способов осуществления несанкционированного доступа к системе, как правило, с использованием чужого имени; подбором паролей; изменением адресов устройств; использованием информации, оставшейся после решения задач; модификацией программного и информационного обеспечения, хищением носителей информации; установкой аппаратуры записи и т. д.

ПОДДЕЛКА ВЫХОДНОЙ ИНФОРМАЦИИ-

- подделка информации может преследовать различные цели. Итогом подделки является то, что конечному потребителю информации будут предоставлены недостоверные данные. Примером могут служить подтасовка результатов выборов или же хищение различного вида товаров, путем ввода в программу фальшивых данных; подделка, изготовление или сбыт поддельных документов, штампов, печатей и бланков; изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов.

НЕСАНКЦИОНИРОВАННОЕ КОПИРОВАНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ-

- в процессе работы каждой компании неизбежны случаи утечки конфиденциальной информации. Несмотря на то, что защитные системы, отвечающие за хранение и доступ к внутренней информации, постоянно совершенствуются, проблема продолжает существовать. Организации несут огромные потери из-за несанкционированного распространения конфиденциальной информации. Несанкционированное копирование может осуществляться посредством изъятия средств компьютерной техники; перехвата информации; несанкционированного доступа к технике, а также манипуляции данными и управляющими командами.

Всем уже давно известно, что неразглашение внутренней информации совсем неэффективно. Необходимо применять меры, основной составляющей которых является защита компьютеров, принадлежащих компаниям, от несанкционированного копирования и выведения данных.

- Необходимо внедрять программы с помощью которых производится мониторинг всех действий, осуществляемых на компьютерах сотрудников фирмы.Необходимо отслеживать любые движения корпоративных данных, их копирование и вывод на внешние носители. Таким образом, службы безопасности компаний имеют возможность моментально реагировать и пресекать любые несанкционированные действия, связанные с копированием информации.
- Ошибки в работе и выход из строя компьютерных систем могут привести к тяжелым последствиям, вопросы компьютерной безопасности становятся наиболее актуальными на сегодняшний день. Известно много мер, направленных на предупреждение преступления. Необходимо наиболее эффективно использовать всевозможные подходы к сохранению конфиденциальной информации с целью сохранения информационной целостности организации.

МЕРЫ БЕЗОПАСНОСТИ

- ***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 сигнализации и многое другое.

- ***К организационным мерам*** отнесем охрану вычислительного центра, тщательный подбор персонала, наличие плана восстановления работоспособности центра после выхода его из строя, универсальность средств защиты от всех пользователей (включая высшее руководство), возложение ответственности на лиц, которые должны обеспечить безопасность центра и т. д. 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 правовым мерам*** относятся также вопросы общественного контроля за разработчиками компьютерных систем и принятие международных договоров об их ограничениях, если они влияют или могут повлиять на военные, экономические и социальные аспекты жизни стран, заключающих соглашение.

Залог успеха предотвращения компьютерной преступности заключается в реализация всех перечисленных выше мер и методов защиты информации и программных средств. Все данные меры позволят решить проблему незаконного доступа и помешают злоумышленнику завладеть чужими конфиденциальными реквизитам.