Защита собственной информации от несанкционированного доступа

Автор: Почивалова Т.С (11 класс)
Науч-ный рук-тель: Мухина И.А

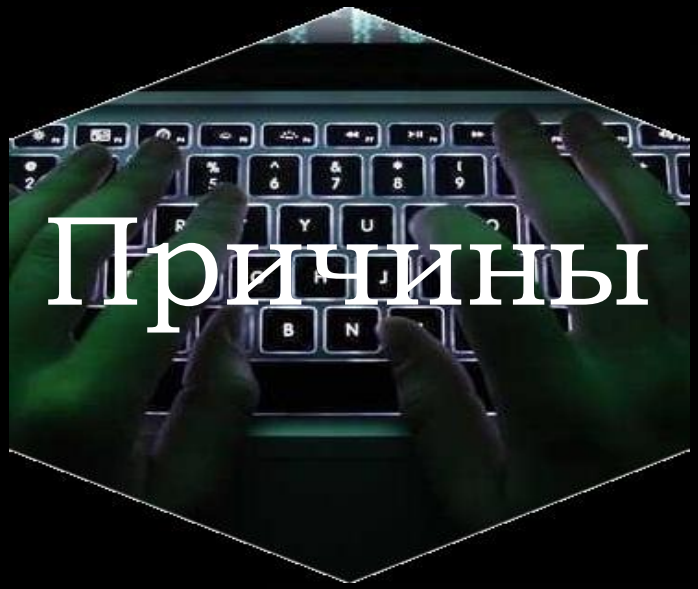
Проблема защиты информации сейчас очень актуальна. Киберпреступность набирает обороты. Среднегодовой ущерб от кибератак в мире составляет $15 млн на организацию.

Что же такое несанкционированный доступ?

Под несанкционированным доступом, если говорить обычным языком, понимается **доступ к информации со стороны лиц, не имеющих прав (полномочий) на доступ к этой информации.** Один из видов преступлений с вмешательством в работу компьютера.

Ошибки конфигурации (прав доступа, файрволов, ограничений на массовость запросов к базам данных)

Ошибки в программном обеспечении



Использование клавиатурных шпионов, вирусов и троянов на компьютерах с маркером доступа

Слабая защищённость средств авторизации (хищение паролей, смарт-карт, физический доступ к плохо охраняемому оборудованию и д.р)

Типовые пути несанкционированного получения информации

· Хищение носителей информации и производственных отходов

· Копирование носителей информации с преодолением мер защиты

· Маскировка под зарегистрированного пользователя

· Мистификация (маскировка под запросы системы)

· Использование недостатков операционных систем и языков Программирования

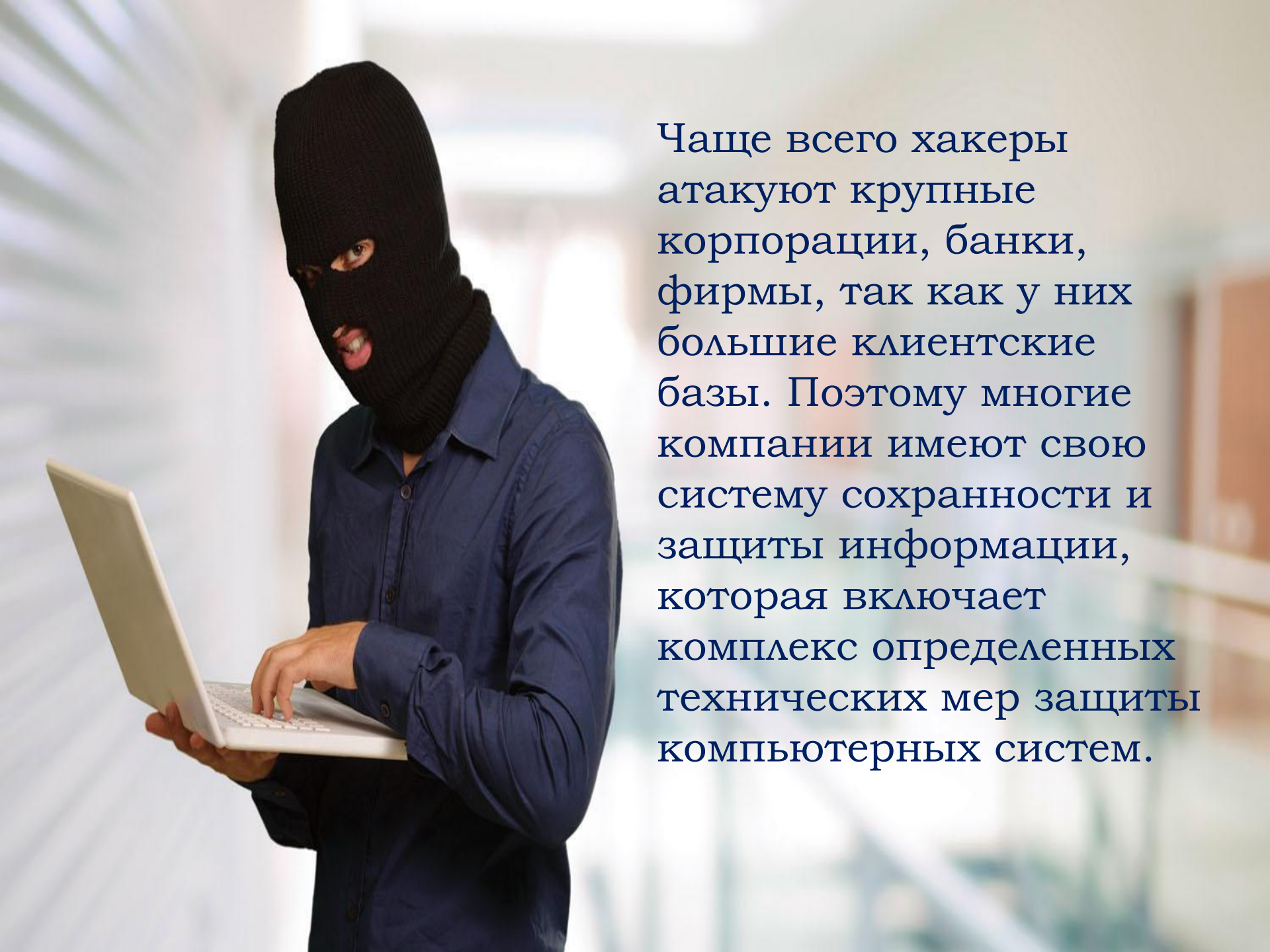
· Использование программных закладок и программных блоков типа "троянский конь«

· Дистанционное фотографирование

· Применение подслушивающих устройств

Что такое защита информации?

Защита информации –
комплекс мер, предназначенных на безопасное хранение и защиту информации от нежелательных пользователей.



Чаще всего хакеры атакуют крупные корпорации, банки, фирмы, так как у них большие клиентские базы. Поэтому многие компании имеют свою систему сохранности и защиты информации, которая включает комплекс определенных технических мер защиты компьютерных систем.

Технические меры по защите информации:

1. Аутентификация пользователей.
Использование уникальных паролей для входа в систему или устройств для идентификации личности по биометрической информации.

2. Защита пароля.
Внедрение мер защиты при администрировании паролей, и ознакомление пользователей с наиболее общими ошибками, позволяющими совершиться компьютерному преступлению.

3. Процедуры авторизации.
Доступа к информации и приложениям, получение пароля с разрешения тех или иных начальников.

5. Защита носителей информации (исходных документов, лент, картриджей, дисков, распечаток).

· вести, контролировать и проверять реестры носителей информации

· обучать пользователей правильным методам очищения и уничтожения носителей информации

· не давать носители информации с критической информацией неавторизованным людям

· обеспечить безопасность распечаток паролей и другой информации, позволяющей получить доступ к компьютеру.

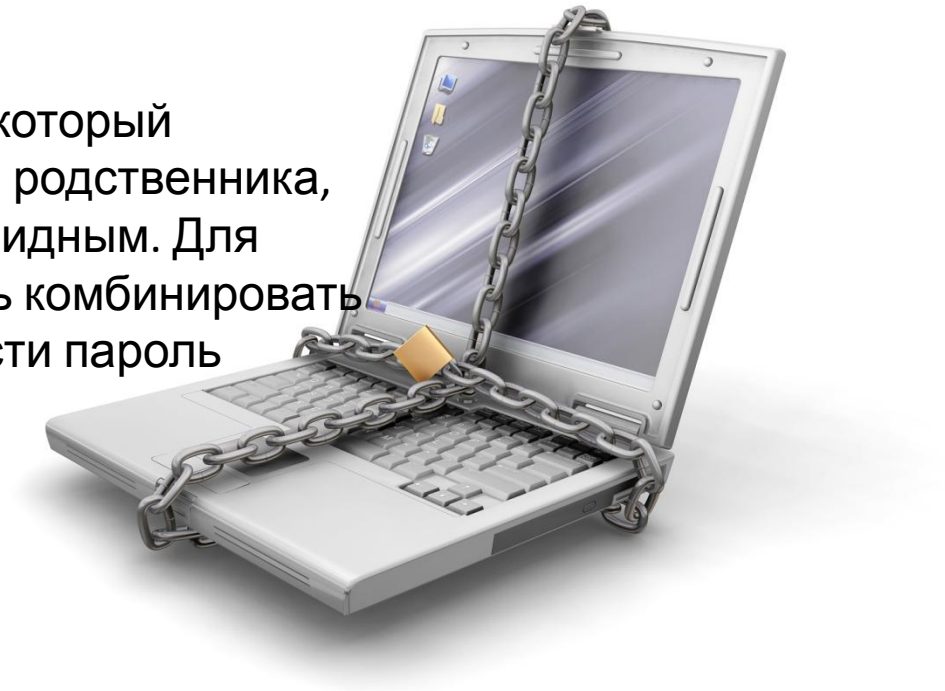
6. Резервное копирование.

Одним из ключевых моментов, обеспечивающих восстановление системы при аварии, является резервное копирование рабочих программ и данных.

Какие меры можно применить обычному пользователю для предотвращения взлома и кражи информации?

1.Используйте шифрование.
С помощью специальных программ можно зашифровать свой жесткий диск, любое внешнее устройство хранения информации, также беспроводную сеть Wi-Fi, и тогда, если злоумышленник захочет вас взломать, сделать он этого не сможет, так как ему будет необходимо знание пароля.

2.Создавайте надежные пароли.
Не рекомендуется использовать пароль, который является адресом, псевдонимом, именем родственника, телефонным номером или чем-либо очевидным. Для создания надежного пароля постарайтесь комбинировать различные цифры, языки, и по возможности пароль должен содержать более 6 символов.



3.Используйте антивирусные программы.

Существует множество вирусов, которые могут попасть на ваш компьютер через Интернет, съемные носители и т.п, и чтобы защитить ваши данные от заражения и последующего удаления информации и пр.(в зависимости от вируса),нужно установить антивирус, благодаря ему можно очистить компьютер от нежелательных программ и восстановить зараженные файлы.

4.Используйте системы, программы, социальные сети, сайты, которые практикуют двухфакторную аутентификацию.

Двухфакторная аутентификация добавляет второй уровень аутентификации при входе в учетную запись. Обычно требуется ввести только имя пользователя и один пароль - это считается однофакторной аутентификацией. 2FA требует от пользователя наличия двух из трех типов учетных данных, прежде чем он сможет получить доступ к аккаунту.

Спасибо за внимание!

"Презентация подготовлена для конкурса "Интернешка«
http://interneshka.org/

Список литературы:

https://ru.wikipedia.org/wiki/Несанкционированный_доступ
http://www.panasenko.ru/Articles/77/77.html
http://www.lessons-tva.info/edu/e-inf3/m3t4_1.html
http://life-prog.ru
http://btimes.ru
http://sosh11.edusluda.ru
http://www.tadviser.ru/index.php/Статья:Киберпреступность_в_мире.