Свердловская область
Горноуральский городской округ
Муниципальное бюджетное общеобразовательное учреждение
средняя общеобразовательная школа № 4
622933, Свердловская обл., Пригородный район, с. Лая, ул. Зеленая площадь, 2,
тел./факс 8(3435)47-88-30, e-mail: ou4laya@mail.ru

ИНДИВИДУАЛЬНЫЙ ОБРАЗОВАТЕЛЬНЫЙ ПРОЕКТ

«Киберпреступления в России»

по предмету «Информатика»

Ученика 9 класса:
Чепуштанова Алексея Леонидовича
Руководитель:
учитель информатики, 1 кк
Пузанова Нина Леонидовна,

с. Лая
2020 г.

Содержание

Введение

В современном мире, в век информации, СМИ и интернета, эта тема как нельзя кстати. Смотря фильмы, сериалы, передачи, мы задались вопросом, а все ли так, как показано на экране? Все ли настолько плохо или настолько хорошо? Стоит ли бояться киберпреступлений нам – обычным людям? И если да, то, как от них уберечься, защититься?

Еще Александр Суворов говорил «Предупрежден – значит вооружен».

Социологические опросы в разных странах, и в первую очередь в высокоразвитых, показывают, что киберпреступность занимает одно из главных мест среди тех проблем, которые тревожат людей.

Объект исследования: киберпреступления.

Предмет исследования: правила профилактики и борьбы с киберпреступлениями.

Цель работы:

изучение проблемы развития киберпреступности в России и нахождение способов ее профилактики.

Задачи:

1. Рассмотреть понятие киберпреступность и виды киберпреступлений.
2. Найти примеры киберпреступлений в мире, России.
3. Дать рекомендации противостояния хакерам в домашних условиях.

Методы исследования:

- изучение научно-популярной литературы по данной проблеме;
- анализ и синтез полученной информации;
- анализ правовой базы;
- анализ статистических данных;
- систематизация и обобщение, выводы по проблемному вопросу.

Гипотеза:

Киберпреступность может перерасти в более глобальную проблему и стать серьёзней бытовых преступлений.

Практическая значимость результатов исследования может быть использована на уроках для передачи полученных знаний обучающимся, с целью расширения их кругозора в области информатики и права; педагогам, для использования научных данных в своих разработках внеклассных мероприятий и для воспитания в подрастающем поколении культуры поведения в сетевом пространстве, методах профилактики правонарушений.

Киберпреступность: понятие, виды, способы [4]

Киберпреступностью является любая преступная активность, где объектом в качестве цели и/или инструмента является компьютер или сетевое устройство.

В некоторых киберпреступлениях осуществляются прямые атаки на компьютеры или другие устройства с целью вывода из строя. В других – компьютеры используются в своих целях киберпреступниками для распространения вредоносных программных кодов, получения незаконной информации, или для получения криптовалюты.

Разделить киберпреступления на отдельные категории не так просто, поскольку существует множество пресечений, однако в целом можно выделить следующие виды киберпреступлений:

1. Финансово-ориентированные киберпреступления.

Немудрено, что многие киберпреступники используют интернет с целью получения коммерческой выгоды, осуществляя следующие типы атак:

- фишинг

Кибермошенники любят собирать низко висящие фрукты, когда предоставляется возможность заразить компьютеры ничего не подозревающих жертв. В подобных схемах излюбленным средством злоумышленников является электронная почта. Суть метода заключается в принуждении получателя письма к переходу по ссылке от имени легитимной организации (банка, налоговой службы, популярного интернет магазина и т. д.). В подобных случаях целью, зачастую, является овладение банковскими данными.

- кибервымогательство

Еще один популярный метод финансово-ориентированного киберкриминала – вымогательство. Как правило, вначале у пользователя или компании, после загрузки вредоносного кода шифруются файлы, а затем поступает предложение о восстановлении в обмен на денежное вознаграж-

дение (обычно в виде биткоинов или другой криптовалюты). Так как государственные денежные знаки можно отследить, а криптовалюту отследить сложно.

- финансовое мошенничество.

Большинство изощренных схем финансового мошенничества связано со взломом компьютерных систем операторов розничной торговли с целью получения банковских данных о покупателях (так называемые целевые атаки) или последующими манипуляциями полученной информацией. Некоторые типы мошенничества, связанного с финансами, чрезвычайно сложно обнаружить.

2. Киберпреступления, связанные со вторжением в личную жизнь

Существует несколько типов подобных киберпреступлений, целью которых является кража личной конфиденциальной информации. Хотя зачастую злоумышленниками движет более глубокая мотивация (например, денежная или связанная с изменение политических настроений), основное внимание сосредоточено на обходе законов и поиске брешей в технологиях, которые защищают персональные конфиденциальные сведения.

- кража персональных данных

Кража личной информации обычно происходит с целью последующей подмены личности человека или группы людей. Хотя некоторые злоумышленники крадут паспорта или другие удостоверения личности для физической подмены личности, в основном кража персональных данных происходит исключительно в интернете.

Например, некто, желающий получить банковский заем, может украсть персональную информацию человека с хорошей кредитной историей.

- шпионаж

Целью шпионажа, начиная от взломов индивидуальных компьютеров или устройств и заканчивая нелегальной массовой слежкой, является тайное отслеживание нашей личной жизни. Здесь может быть как физиче-

ский шпионаж (например, при помощи веб- или CCTV-камер для наблюдения за отдельными персонами или группой людей), так и массовый мониторинг различного рода коммуникаций (чтение почты, текстовых сообщений мессенджеров, смс и так далее).

3. Нарушение авторского права

Нарушение авторских прав – одна из наиболее распространенных форм киберпреступлений. В первую очередь в эту категорию попадает выкладка в общий доступ музыки, фотографий, фильмов, книг и т. д. без согласия авторов.

Спам – чрезвычайно распространенный и многовариантный тип киберпреступлений. Сюда входит массовая рассылка по электронной почте, смс, мессенджерам и другим каналам коммуникации. Любую рассылку без согласия получателей можно отнести к спаму.

4. Социальные и политически мотивированные киберпреступления

Некоторые типы киберпреступлений направлены на изменения настроений в политической среде или нанесение намеренного вреда или снижения влияния отдельных личностей или группы людей.

5. Преступления на почве ненависти и домогательства

Преступления на почте ненависти по отношению к личности или группе людей обычно совершаются на основе гендерной, расовой, религиозной, национальной принадлежности сексуальной ориентации и других признаков. Примеры: домогательства и рассылка оскорбительных сообщений и вброс ложных новостей, касающихся определенной группы лиц.

Анонимность и легкодоступность интернета серьезно затрудняют борьбу с преступлениями на почве ненависти.

6. Терроризм.

Группировки экстремистской направленности и воинственные народы все чаще используют киберпространство для запугивания, распространения пропаганды и иногда нанесения вреда IT-инфраструктурам. Увели-

чения количества бизнесов, служб и устройств, доступных через интернет, несомненно будет и провоцировать новые случаи кибертерроризма.

7. Кибербуллинг

Использование компьютеров и подключенных устройств для домогательств, унижения и запугивания личностей подпадает под категорию кибербуллинга. Граница между кибербуллингом и некоторыми формами преступлений на почве ненависти зачастую размыта. Некоторые формы кибербуллинга (например, вброс обнаженных фотографий) могут подпадать под незаконные действия (например, эксплуатация детей).

8. Киберпреступления, связанные с недозволенными действиями

Изнанка интернета, именуемая также «dark web» (или глубоким интернетом), используется для совершения разного рода противоправных действий.

9. Противозаконная порнография

Распространение порнографии через интернет во многих странах трактуется как киберпреступление, в других – происходит лишь запрет содержимого экстремистской направленности. Распространение изображений с детской порнографией запрещено в большинстве стран.

10. Груминг

Сетевой груминг связан с сексуальными домогательствами до несовершеннолетних. В процессе могут использоваться различные методы общения: смс, социальные сети, электронная почта, чаты (например, в онлайн играх) и форумы. Во многих странах груминг подпадает под категорию киберпреступлений.

11. Распространение наркотиков и оружия

Различные IT-решения, используемые для распространения легитимных товаров и служб, могут также использоваться злоумышленниками. Например, рынки даркнета, существующие во всемирной паутине, помогают контрабандистам продавать оружие и наркотики и в тоже время оставаться вне поля зрения правоохранительных органов.

Как же киберприступники совершают свои преступления?

Существует четыре наиболее распространенных способа, которыми пользуются киберпреступники.

Первый, которого боятся многие люди – использование вредоносных программ. Вероятно, вы понимаете, что существует множество методов эксплуатации систем, и насколько важно использоваться различными мерами безопасности, например, устанавливать длинные пароли и делать регулярные обновления. Этот тип атак базируется на злоупотреблении компьютерами и сетями.

Второй способ – DDOS атаки, когда злоумышленник пользуется коммуникационным сетевым протоколом для создания огромного количества запросов к серверу или службе. В этом типе атак главная цель – вывести из строя объект воздействия.

Третий способ – комбинация социальной инженерии и вредоносного кода. Наиболее известная форма подобного рода атак – фишинг, когда жертву принуждают к определенным действиям (нажатию на ссылку в электронном письме, посещению сайта и т. д.), что впоследствии приводит к заражению системы при помощи первого метода.

Четвертый способ – незаконная деятельность: домогательства, распространение незаконного контента, груминг и т. д. В этом случае злоумышленники скрывают свои следы посредством анонимных профайлов, шифрованных сообщений и других подобных технологий.

Киберпреступления в России в 2020 году [5]

1. Хакеры взломали почту псковского митрополита и требуют выкуп в 10 млн рублей.

2 мая 2020 года стало известно о взломе электронной почты митрополита Псковского и Порховского Тихона (Шевкунова), который также является председателем Патриаршего совета по культуре и членом Совета при президенте РФ по культуре и искусству. Хакеры требуют выкуп в размере 10 млн рублей за возвращение доступа к сообщениям.

2. Полицейские в Подмосковье создали онлайн-магазин по торговле наркотиками.

В конце апреля 2020 года Следственный комитет России сообщил о задержании в Московской области пятерых сотрудников полиции, которых подозревают в торговле наркотиками через интернет — они сбывали запрещенные вещества через канал в Telegram, которые сами и создали.

3. Переходя на удаленку, компании открывают хакерам доступ к своим серверам.

Из-за спешного массового перехода компаний на удаленную работу стремительно растет число корпоративных серверов, доступных для злоумышленников из интернета – сообщили 27 марта 2020 года эксперты центра мониторинга и реагирования на киберугрозы Solar JSOC. Одна из главных причин – применение компаниями незащищенного протокола удаленного доступа RDP (Remote Desktop Protocol). По данным Solar JSOC, всего за одну неделю количество устройств, доступных из интернета по протоколу RDP, выросло на 15% в России (общее число на сегодня более 76 тыс. единиц) и на 20% в мире (более 3 млн единиц).

Если ИТ-служба компании не уделяет должного внимания безопасности удаленного доступа, корпоративный сервер становится крайне уязвимым для злоумышленников. Например, нередки ситуации, когда удаленный сервер доступен и виден из сети Интернет – любой желающий может попробовать подключиться к нему. При этом злоумышленник может

обмануть систему идентификации и аутентификации, подобрав пароль, осуществив подмену сертификата или использовав уязвимости RDP.

4. ФСБ задержала 30 торговцев данными кредитных карт и изъяла у них слитки золота

24 марта 2020 года Федеральная служба безопасности (ФСБ) России сообщила о задержании хакерской группировки, занимавшейся торговлей краденых банковских карт.

Киберпреступники создали свыше 90 интернет-магазинов по продаже похищенных данных, которые впоследствии использовались для хищения денежных средств с банковских счетов граждан различных государств, в том числе путем приобретения дорогостоящих товаров в интернете.

5. Кибермошенники пользуются эпидемией и атакуют россиян от имени госструктур

19 марта 2020 года стало известно об увеличения количества мошеннических схем в рунете из-за распространения коронавируса. Одна из них заключается в рассылке фейковых писем, в том числе с доменов, похожих на адреса госструктур.

Уголовная ответственность за совершение киберпреступлений [2]

Преступления в сфере компьютерной информации регламентирует Глава 28 Уголовного кодекса Российской Федерации.

Статья 272. Неправомерный доступ к компьютерной информации
(в ред. Федерального закона от 07.12.2011 N 420-ФЗ)

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации,

- наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности,

- наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.

(в ред. Федерального закона от 28.06.2014 N 195-ФЗ)

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, - наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничени-

ем свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления,

- наказываются лишением свободы на срок до семи лет.

Примечания. 1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ (в ред. Федерального закона от 07.12.2011 N 420-ФЗ)

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации,

- наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности,

- наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления,

- наказываются лишением свободы на срок до семи лет.

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

(в ред. Федерального закона от 07.12.2011 N 420-ФЗ)

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб,

- наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления,

- наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.

Как не попасть на «крючок» киберпреступника

Первоочередные шаги для повышения безопасности [1]:

1. Регулярно скачивайте обновления для программного обеспечения, часть атак идёт через неисправленные ошибки.
2. Настройте межсетевой экран для фильтрации нежелательных входящих соединений.
3. Установите качественное антивирусное и антишпионское программное обеспечение.
4. Установите спам-фильтр в почтовые программы (например, в Outlook) Не открывайте писем от пользователей, которых вы не знаете.
5. Не переходите по ссылкам на известные сайты (социальные сети, банки, интернет-магазины) непосредственно из писем. Очень часто такие письма являются фишинговыми. Часто посещаемые сайты лучше держать в браузере в закладках. Ну, или каждый раз искать эти сайты в яндексе, гугле.
6. Придумывайте (возможно, с помощью специальных генераторов) надёжные не повторяющиеся пароли.
7. Храните несколько резервных копий важных данных.
8. Обращайте внимание, если ваши знакомые начинают вести себя необычно игнорируйте их просьбы одолжить денег или предоставить другие ресурсы. Лучше уточнить подробности по телефону или лично.

А так же рекомендуем вам использовать 11 простых правил самозащиты от специалистов по кибербезопасности компании Group-IB [3]:

1. К своей основной карте в вашем банке выпустите дополнительную, которой будете расплачиваться в интернете. Туда легко можно будет переводить небольшие суммы денег, и в случае компрометации данных достаточно просто заблокировать ее.
2. Регулярно проверяйте состояние своих банковских счетов, чтобы убедиться в отсутствии «лишних» и странных операций.
3. Храните номер карточки и ПИН–коды в тайне. Запомните и сотрите/заклейте CVC-код

4. Используйте виртуальные карты, которые сейчас предоставляют платежные системы.

5. Поставьте лимит на сумму списаний или перевода в личном кабинете банка.

6. Будьте осмотрительны в отношении писем со вложенными картинками, поскольку файлы могут содержать вирусы. Открывайте вложения только от известных вам отправителей. И всегда проверяйте вложения на наличие вирусов, если это возможно.

7. Не переходите необдуманно по ссылкам, содержащимся в спам-рассылках. Удостоверьтесь в правильности ссылки, прежде чем переходить по ней из электронного письма.

8. Не заполняйте полученные по электронной почте формы и анкеты. Личные данные безопасно вводить только на защищенных сайтах.

9. Проверяйте запросы персональных данных из каких-либо деловых и финансовых структур. Лучше обратиться в эти структуры по контактам, указанным на официальном сайте, а не в электронном письме.

10. Насторожитесь, если кроме вас в электронном сообщении указаны другие адресаты. Крайне маловероятно, чтобы при общении с клиентом по поводу личных учетных данных банк ставил кого-то в копию.

11. Насторожитесь, если от вас требуют немедленных действий или представляется чрезвычайная ситуация. Это тоже может быть мошенничеством. Преступники вызывают у вас ощущение тревоги, чтобы заставить вас действовать быстро и неосмотрительно.

Заключение

Киберпреступность и кибертерроризм являются объективным следствием глобализации информационных процессов и появления глобальных компьютерных сетей. С ростом использования информационных технологий в различных сферах деятельности человека растет и использование их в целях совершения преступлений.

Необходимость защиты от киберпреступников очевидна. Желательно, чтобы на уровне государства решались проблемы борьбы с киберпреступлениями, а повсеместно проводить работу по разъяснению ограждения от киберпреступников. Наша безопасность в наших руках! Мы за безопасность использования информационного пространства.

Чем сильнее становится зависимость жизни общества от компьютерных систем, тем опаснее уязвимость России и других стран от всевозможных мастей киберпреступников. О безопасности надо думать сегодня, завтра уже может быть поздно.

Преступления в сфере информационных технологий стали опасными для общественности. Несмотря на то, что компьютерные преступления появились сравнительно недавно, они быстро развиваются. Слабая подготовка правоохранительных органов по расследованию такого рода преступлений и высокий уровень скрытности преступников, способствует развитию киберпреступлениям и привлекает все больше и больше людей.

Киберпреступность сильно отличается от традиционных видов преступлений. Следовательно, порождает ряд проблем по развитию защитных мер от несанкционированного доступа к компьютерной информации, с дальнейшим её использованием и распространением вирусных программ, которые нарушают работу систем. Преступления в сфере информационных технологий привлекательны большому числу преступников своей невероятной выгодностью и безнаказанностью преступных деяний.

Поэтому к вопросу о киберпреступности нужно отнестись очень серьезно. Технологии в современном мире не стоят на месте и быстро раз-

виваются, что дает новые возможности для совершения нового рода киберпреступлений. Правительственным органам нужно довольно серьезно заняться решением проблемы киберпреступности, иначе это может привести к необратимым последствиям.

Таким образом, можно считать, что поставленные цели достигнуты. Мы узнали много нового, интересного и полезного. Полученные знания пригодятся в жизни всем нам.

И еще, если люди во всех странах будут больше знать о разных видах киберпреступлениях, то тогда будет действовать поговорка: «Предупрежден – значит, вооружен» и тогда никто не попадет в лапы мошенников.

Список литературы

1. Маслаков А.С. Особенности киберпреступлений в России. Инструменты нападения и защита информации./Под ред. Мовчан Д.А. – ДМК-Пресс, 2018. – с. 226
2. Гл.28.Уголовная ответственность за киберпреступления: https://szsut.sledcom.ru/Kiberprestupnost/item/1159549/
3. Статья 11 правил сетевой безопасности: как защититься от кибермошенников: https://iecp.ru/articles/item/402805
4. Статья «Киберпреступления: понятия, виды и методы защиты»: https://sys-team-admin.ru/stati/bezopasnost/170-kiberprestupnost-ponyatie-vidy-i-metody-zashchity.html
5. Статья «Киберпреступность и киберконфликты: в России»: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BA%D0%BE%D0%BD%D1%84%D0%BB%D0%B8%D0%BA%D1%82%D1%8B_:_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D1%8F

Приложения

Приложение 1 «Безопасность детей в Интернете»

Приложение 2 «Безопасность подростков в Интрнете»

Основные правила безопасного использования интернета!!!

Установи на свой браузер фильтр или попроси сделать это взрослых – тогда ты сможешь смело путешествовать по интересным тебе страницам. Всегда спрашивай родителей о незнакомых вещах в интернете. Они расскажут, что безопасно делать, а что нет.

Если хочешь скачать картинку или мелодию, но тебя просят отправить смс — не спеши! Сначала спроси у взрослых!

Не скачивай и не открывай неизвестные тебе или присланные незнакомцами файлы из интернета. Чтобы избежать заражения компьютера вирусом, установи на него специальную программу – антивирус! Подробную информацию посмотри на сайте ИТК.РФ или по телефону 22-0-44 или 95-0-30.

Не встречайся без родителей с людьми из интернета в реальной жизни. В интернете многие люди рассказывают о себе неправду.

Общаясь в интернете, будь дружелюбен с другими. Не пиши грубых слов! Ты можешь нечаянно обидеть человека. Читать грубости также неприятно, как и слышать.

Прежде чем начать дружить с кем-то в интернете, спроси у родителей, как безопасно общаться в сети.

Если твой компьютер заблокировался картинкой с требованием отправить смс, срочно сообщи взрослым, позвоните в «Илим-Телеком» по т. 22-0-44 специалисты компании посоветуют как разблокировать твой компьютер!

Никогда не рассказывай о себе незнакомым людям: где ты живешь, учишься, свой номер телефона. Это должны знать только твои друзья и семья! Не отправляй свои фотографии, а также фотографии своей семьи и своих друзей незнакомым людям. Они могут использовать их так, что это навредит тебе или твоим близким.

От нас! Будь внимательней, это поможет тебе обойти многие реальные проблемы.Удачи в глобальных просторах интернета;)