муниципальное бюджетное общеобразовательное учреждение
города Ростова-на-Дону «Школа № 6
имени Героя Советского Союза Самохина Н.Е.»

ИНДИВИДУАЛЬНЫЙ ПРОЕКТ

на тему

“ Киберпреступность”

Выполнил учащийся 11А класса:

Кохреидзе Илья Иванович

Научный руководитель:

Казарова Лаура Варужановна

Допуск к защите: _____

г. Ростов-на-Дону 2024 год

ОГЛАВЛЕНИЕ

Введение

Мы живем XXI веке, который еще называют веком информационных технологий. Мир и жизнь каждого человека изменись с появлением информационных технологий, жизнь в человека стала легче. Сегодня за человека много работы выполняют машины, нас повсюду окружает электроника.

Современное информационное общество подвержено ряду потенциальных угроз, одной из которых является киберпреступность.

Во все времена частная жизнь человека защищалась от проникновения посторонних. В информационном обществе защита личного пространства значительно усложнилась. Технологии и средства дают возможность превратить закрытую систему в прозрачную.

В массивных источниках формируются базы данных, содержащие персональную информацию, это обстоятельство представляет угрозу нарушения частой жизни.

Сегодня одной из престижных и востребованных специальностей является профессия «Специалист по компьютерной кибербезопасности», так как любая компания является потенциальной жертвой кибератак. Чем дороже компания, тем выше риск. А значит тем больше денег готовы тратить руководители компаний на специалиста по кибербезопасности.

Уважающая себя компания не жалеет денег и ресурсов на защиту данных. Согласно статистике за последний год бюджеты на кибербезопасность в российских организациях выросли на 20 %.

С каждым годом число кибератак увеличивается, а злоумышленники совершенствуют вредоносное ПО. Компаниям срочно нужны специалисты, которые смогут оперативно искать уязвимости и предотвращать утечки данных.

Цели работы: исследовать киберпреступность, изучить профилактику киберпреступности и способы борьбы с ней.

Задачи работы:

- сформулировать понятие киберпреступности;
- изучить основные виды киберпреступности;
- узнать, кто такие киберпреступники;
- выявить способы профилактики киберпреступности и способы борьбы с ней;
- определить методы обеспечения защиты от киберпреступности для себя и своих близких.

Объект исследования: киберпреступность, ее виды и особенности.

1.1. Понятие о киберпреступности

Что такое киберпреступность?

Киберпреступность – это преступная деятельность, в рамках которой либо атакуются компьютер, компьютерная сеть или сетевое устройство. Большинство кибератак совершается киберпреступниками или хакерами с целью получения финансовой прибыли. Однако целью кибератак может быть и выведение компьютеров или сетей из строя – из личных или политических мотивов.

Киберпреступления совершают частные лица и организации – от начинающих хакеров до слаженных группировок, которые используют продвинутые методики и хорошо подкованы технически.

1.2. Категории киберпреступлений

Существует три основные категории кибер-преступлений: индивидуальные, имущественные и государственные. Типы используемых методов и уровни сложности варьируются в зависимости от категории.

Имущественная: Это похоже на случай из реальной жизни, когда преступник незаконно завладел банковскими данными или данными кредитной карты физического лица. Хакер крадет банковские реквизиты человека, чтобы получить доступ к средствам, совершить онлайн-покупки или провести фишинговые аферы, заставляющие людей предоставлять ему свою персональную информацию. Они также могут использовать вредоносное программное обеспечение для получения доступа к веб-странице с конфиденциальной информацией.

Индивидуальная: Эта категория кибер-преступлений привлекает жертву (человека) для распространения вредоносной или незаконной информации в Интернете. Жертва может быть вовлечена в такие незаконные действия, как кибersталкинг, распространение порнографии и торговля людьми.

Правительственная: Это наименее распространенная категория кибер-преступности, но это самое серьезное преступление. Преступление против правительственных органов также известно как кибер-терроризм. Правительственная кибер-преступность подразумевает взлом веб-сайтов правительственных и военных учреждений или распространение пропаганды. Такие преступники обычно являются террористами или представителями правительственных органов вражеских стран

2.1. Кто такие киберпреступники?

Киберпреступники — это люди или группы лиц, которые совершают незаконные злонамеренные действия с использованием компьютеров или киберпространства.

Их основная цель — изменить или заразить данные в своих корыстных интересах. Они делают это благодаря своим знаниям о человеческом поведении, навыкам работы с компьютером и различным методам, таким как межсайтовый скриптинг, для получения несанкционированного доступа в сети своей жертвы.

В большинстве случаев киберпреступники не выбирают конкретную жертву в качестве своей добычи. Вы можете стать мишенью, если нажмете на неизвестные ссылки, разгласите свою конфиденциальную информацию в Интернете или загрузите вредоносные файлы с нелицензионных сайтов.

Во-первых, хакеры могут быть любыми людьми. Это могут быть программисты, которые раньше работали в компаниях по разработке программного обеспечения, но потом перешли на темную сторону. Также это могут быть студенты, которые пытаются проверить свои навыки взлома на слабо защищенных сайтах. К сожалению, некоторые из них используют свои знания и навыки для незаконных целей.

Во-вторых, в последнее время все больше и больше киберпреступников имеют свои цели и мотивы. Некоторые из них пытаются получить конфиденциальную информацию о компаниях, чтобы использовать ее в своих интересах. Другие просто хотят нарушить работу сайта или компьютерной системы из-за простой жажды разрушения. Есть также и те, кто хочет вымогать деньги, запугивая жертву.

В-третьих, существует различная категоризация киберпреступников. Некоторые из них, так называемые белые хакеры, работают на компании, проверяя их защищенность, и находят и исправляют уязвимости. Серые хакеры могут использовать свои навыки как для добрых, так и для злых целей. Наконец, черные хакеры – это те, кто используют свои навыки только для незаконных целей.

Киберпреступники используют различные методы для своих атак. Они могут использовать социальную инженерию, чтобы обмануть пользователей и получить доступ к их учетным записям или использовать различные виды вредоносного программного обеспечения (малварь), такие как вирусы, трояны или шпионское ПО. Кроме того, они могут использовать такие методы, как фишинг, перехват пакетов, атаку на уязвимости в программном обеспечении и многие другие.

2.2. Виды киберпреступлений

В условиях постоянно развивающихся цифровых технологий широкий спектр киберугроз может иметь серьезные последствия для бизнеса, если не защитить его должным образом. Понимание различных типов киберпреступлений (начиная с вредоносных программ и программ-вымогателей и заканчивая фишингом и кражей личных данных) – является первым шагом для обеспечения безопасности своей компании.

1. Фишинг

Фишинг – это один из наиболее распространенных способов кражи личной информации пользователей. Фишинговые практики обычно состоят в том, что киберпреступники притворяются законными представителями той или иной организации, чтобы получить конфиденциальные данные жертв, такие как пароли и номера кредитных карт.

Фишинговые электронные письма обычно составляются таким образом, чтобы быть похожими на официальные имейлы от различных финансовых учреждений, налоговой службы или других организаций с целью обманом заставить людей предоставить свою личную информацию.

Подобные мошеннические практики обычно включают в себя отправку электронных писем или телефонные звонки, информирующие получателей о том, что они должны немедленно обновить информацию о своей учетной записи, иначе рискуют быть заблокированными. Этот тип мошенничества стал очень популярным в последние несколько лет, потому что преступника трудно отследить, а сама практика – не сложная. Компания Wandera, занимающаяся IT-безопасностью, утверждает, что новый фишинговый сайт создается каждые 20 секунд.

Таким образом, в минуту создается три новых фишинговых веб-сайта, подвергающих бизнес потенциальным угрозам. Лучший способ не стать жертвой – это рассказать сотрудникам о признаках фишинговых писем и разработать политику безопасности в отношении того, что работники должны делать, если они подозревают, что электронное письмо может быть фальшивкой.

2. Взлом (хакерство)

Хакинг – это акт получения несанкционированного доступа к компьютерной системе с целью заражения ПК жертвы или обхода мер безопасности. Хакеры – это те, кто используют свои знания для обнаружения уязвимостей в компьютерной системе. Как итог, компании могут столкнуться с различными проблемами (начиная со взлома компьютерной системы и заканчивая получением доступа к конфиденциальным данным).

Хакеры могут даже разрушить репутацию компании, опубликовав конфиденциальную информацию о ней. Порой их называют хактивистами (англ. «hacktivists»). Существует 3 типа хакеров: белая шляпа, черная шляпа и серая шляпа.

Хакеры «в белых шляпах» (англ. «white hat hackers») используют свои навыки, чтобы находить ошибки в программном обеспечении раньше, чем это сделают злоумышленники – они сообщают об ошибках, чтобы их можно было быстрее исправить.

Хакеры «в черных шляпах» (англ. «black hat hackers») создают программы, предназначенные для взлома компьютеров других пользователей, кражи информации и продажи ее в Dark Web.

Хакеры «в серых шляпах» (англ. «grey hat hackers») используют методы, которые находятся между двумя этими крайностями – они пытаются выявить уязвимости в системе, но подобные практики могут нарушать законы или этические стандарты.

3. Криптоджекинг

Криптоджекинг – это тип киберпреступления, при котором хакеры незаконно используют компьютеры и сети людей для получения криптовалюты. Согласно данным SonicWall, глобальный объем криптоджекинга увеличился до 66,7 млн в первой половине 2022 года, что на 30% больше, чем в первой половине 2021 года. Рост на 269% сильнее всего повлиял на финансовую отрасль.

Одной из основных проблем криптоджекинга является чрезмерная нагрузка на процессор, что приводит к значительному замедлению работы систем или даже полному сбою. Иногда это происходит до того, как компании осознают, что было осуществлено киберпреступление. Организации могут защитить себя от такого рода преступлений, попросив ИБ-специалиста периодически проверять систему на предмет необычных скачков нагрузки процессора.

4. Спуфинг

Спуфинг – это такой тип киберпреступности, когда кто-то изменяет свою личность в Интернете, чтобы обмануть другого пользователя. Эти преступления могут включать в себя подмену электронной почты, номера телефона, профиля в социальных сетях и рекламу. Один из ярких примеров – когда хакер отправляет электронное письмо, которое маскируется под имейл от коллеги по работе, и запрашивает конфиденциальную информацию о компании.

Киберпреступники также могут создавать веб-страницы, которые внешне похожи на официальные сайты различных компаний, но предназначены для сбора личной информации. Лучший способ избежать этих мошеннических практик – проверять ссылки, прежде чем переходить по ним или указывать какие-либо данные. Следует быть осторожным с нежелательными электронными письмами, в которых запрашивается пароль, номера финансовых счетов или другая конфиденциальная информация пользователя.

5. Программы-вымогатели

Программа-вымогатель – это разновидность вредоносного ПО, которое атакует компьютерные системы, блокирует данные и требует оплаты за их разблокировку. Как только компьютер заражен программой-вымогателем, пользователю предлагается заплатить выкуп, чтобы получить ключ дешифрования, необходимый для восстановления контроля над данными.

Средняя стоимость атаки с использованием программы-вымогателя составляет более 4 миллионов долларов, в то время как деструктивная атака в среднем превышает 5 миллионов долларов. Заражение программами-вымогателями часто можно предотвратить, соблюдая основные правила безопасности, такие как обновление операционной системы или отказ от перехода по подозрительным ссылкам или вложениям от неизвестных отправителей.

6. Межсайтовый скриптинг

Межсайтовый скриптинг (XSS) – это уязвимость веб-безопасности, которая возникает, когда злоумышленник внедряет вредоносные скрипты на доверенный веб-сайт или в веб-приложение. XSS позволяет злоумышленникам получить контроль над сеансом пользователя, украсть его учетные данные и собрать ценную информацию о компании.

Например, злоумышленники могут разместить вредоносный код на скомпрометированном сайте, который только и ждет момента, когда ничего не подозревающий пользователь войдет в систему, чтобы получить конфиденциальную информацию с компьютера жертвы. Эти уязвимости иногда позволяют злоумышленникам перехватывать сеанс и полностью выдавать себя за жертву.

Существует три типа XSS — Stored XSS, Reflected XSS и DOM-based XSS (Document Object Model).

Stored XSS. Злоумышленники используют этот тип эксплойта для загрузки вредоносного ПО или кражи файлов cookie с конфиденциальной личной информацией, такой как пароли и номера кредитных карт.

Reflected XSS. Запускается, когда жертва нажимает на ссылку внутри скомпрометированного сайта, который активирует скрипт в браузере, содержащий вредоносный код. Браузер жертвы отправит скрипт обратно на атакующий сервер.

DOM-based XSS. Использует уязвимости в DOM или в том, как браузеры анализируют HTML-документы. Цель этой атаки – заставить браузер вносить изменения, создающие уязвимости, путем манипулирования объектами JavaScript, такими как XMLHttpRequest или WebSocket.

Чтобы защитить себя от всех трех типов межсайтового скриптинга, компаниям необходимо внедрить безопасные методы кодирования, такие как линтинг, и обеспечить надлежащую проверку входных значений.

7. Кража личности

Кража личности – это тип киберпреступления, при котором человек использует чужие личные данные, такие как имя и номер социального страхования, номер банковского счета и информацию о кредитной карте, для совершения мошенничества. Плохие «актеры» могут запятнать хорошую репутацию жертвы и испортить ее кредитную историю.

Хакеры собирают информацию о пользователях различными методами, включая взлом компьютера, кражу почты, камеры для захвата данных с экранов ПК и создание поддельных копий удостоверений личности ничего не подозревающих жертв. Затем киберпреступники используют эту информацию, чтобы выдавать себя за жертв, подавать заявки на получение займов, брать под контроль финансы людей, получая доступ к их банковским счетам.

Чтобы избежать кражи личных данных, следует должным образом следить за документами, содержащими конфиденциальную информацию: разрезать их на кусочки, прежде чем выбрасывать; не пользоваться общественными урнами.

8. Мошенничество в сфере кредитования

При мошенничестве в сфере кредитования преступник выдает себя за представителя компании и запрашивает оплату за товары или услуги, которые никогда не были предоставлены. Эти мошенничества, как правило, успешны, потому что поддельный счет-фактура отправляется в бухгалтерию, которая не знает поставщика лично.

Предприятия наиболее уязвимы для такого рода мошенничества при масштабировании операций и переходе от небольшой компании к среднему или крупному бизнесу. Преступник может выдавать себя за сотрудника, запрашивающего средства от имени компании, или даже зайти так далеко, что будет создавать поддельные счета-фактуры, которые кажутся законными.

Если речь идет о киберпреступлениях, то компаниям необходимо иметь систему сдержек и противовесов, полагаясь на нескольких сотрудников внутри организации, например, требуя нескольких подписей для всех платежей, превышающих определенную сумму.

9. Вредоносные программы

Вредоносные программы – это хакерское ПО, предназначенное для нарушения работы компьютера, сбора конфиденциальной информации или получения удаленного доступа. Вредоносные программы часто остаются незамеченными, их трудно удалить, и они могут нанести значительный ущерб компьютерным системам, заражая файлы, изменяя данные и уничтожая системные утилиты.

Важно отметить, что вредоносное ПО может маскироваться под обычное программное обеспечение, чтобы ему было проще попасть на

компьютер жертвы. Примерами подобных программ являются вирусы, черви, трояны, шпионское и рекламное ПО.

10. Социальная инженерия.

Социальная инженерия – это искусство манипулирования людьми с целью получения конфиденциальной информации или учетных данных. Данная практика включает в себя «маскировку» под сотрудника компании, совершение телефонных звонков, отправку электронных писем и использование служб мгновенного обмена сообщениями, чтобы завоевать доверие жертвы.

Преступник запрашивает такую информацию, как пароли и личные идентификационные номера (PIN-коды). По статистике, 98% всех киберпреступлений связаны с той или иной формой социальной инженерии.

Жертв не только обманом заставляют выдать свою личную информацию, но они также могут невольно раскрыть коммерческие тайны и поделиться интеллектуальной собственностью компании. Наличие плана реагирования на подобные инциденты будет иметь большое значение для предотвращения такого рода преступлений.

11. Мошенничество с техподдержкой

В этих аферах мошенник выдает себя за представителя известной компании и звонит потенциальным жертвам, утверждая, что обнаружил угрозы на их ПК. Эти угрозы могут включать в себя разное: от вредоносных программ до вирусов, которые можно устранить за определенную плату.

Затем он обманом заставляет предоставить удаленный доступ к системе, что позволяет мошеннику требовать еще больше денег или украсть личную информацию. ФБР сообщает, что супружеская пара из штата Мэн потеряла 1,1 миллиона долларов после получения всплывающего предупреждения о том, что их компьютер был взломан и была предпринята попытка скомпрометировать их банковскую информацию.

Мошенники нацелены на людей, находящихся в стрессовых ситуациях, которые уязвимы и готовы заплатить что угодно, чтобы защитить себя. Жертвы могут не осознавать, что их обманули, пока не станет слишком поздно, потому что мошенник предоставил им обновления программного обеспечения, которые позволили им поверить, что они в безопасности. Мошенники убедили супружескую пару перевести деньги со своего пенсионного счета, прежде чем прервать с ними всякую связь.

12. Взлом IoT-устройств

Взлом IoT-устройств является одной из наиболее распространенных форм киберпреступности. Этот взлом происходит, когда хакер использует устройство, подключенное к Интернету, такое как умный термостат или холодильник. Он взламывает устройство и заражает его вредоносным ПО, распространяясь по всей сети.

Хакеры используют зараженные системы для запуска атак на другие системы в сети. Эти атаки часто могут привести к краже данных с устройств и предоставить мошенникам доступ к конфиденциальной информации. Риск взлома IoT-устройств возникает из-за того, что девайсы имеют ограниченный уровень безопасности, вычислительную мощность, память и объем хранилища. Это означает, что они с большей вероятностью будут иметь уязвимости, чем другие системы.

13. Компьютерное пиратство

Компьютерное пиратство – это акт незаконного копирования, распространения или использования программного обеспечения без права собственности или законного разрешения. Это может произойти путем загрузки программ с нелегального веб-сайта, копирования ПО с одного компьютера на другой или продажи его копий.

Пиратское программное обеспечение влияет на прибыль компании, не позволяя ей зарабатывать деньги на своих продуктах. Исследование Software Alliance показало, что 37% программного обеспечения, установленного на персональных компьютерах, является нелицензионным или пиратским. Поскольку это глобальная проблема, компаниям важно понимать, как они могут пострадать и какие существуют методы самозащиты.

14. Трояны

Троянская программа – это вирус, который маскируется под обычную программу и устанавливается на компьютер без разрешения пользователя. При запуске он может выполнять такие действия, как удаление файлов, установка других вредоносных программ и кража информации, такой как номера кредитных карт.

Ключ к предотвращению подобной мошеннической деятельности является загрузка программ только с авторитетных сайтов, таких как сайт компании или авторизованных партнеров.

15. Подслушивание (англ. «Eavesdropping»)

Подслушивание – это тайное прослушивание или запись разговора без ведома и/или согласия сторон. Это может происходить по телефону, с помощью скрытой камеры или даже через удаленный доступ к системе.

Данная практика является незаконной и подвергает пользователя риску мошенничества и кражи личных данных. Человек может защитить свою компанию, ограничив ту информацию, которой сотрудники делятся по электронной почте. Шифрование разговоров и использование специального программного обеспечения, которое предотвращает удаленный доступ неавторизованных пользователей к сетевым ресурсам, также будут эффективными средствами защиты.

16. DDoS-атаки

DDoS-атаки (Distributed Denial of Service) нацелены на службу или систему, которую заваливает большим количеством запросов, чем она может обработать. Бесконечный поток запросов вынуждает серверы отключаться, нарушая доступность информации для пользователей, пытающихся получить к ней доступ.

Хакеры используют DDoS как форму протеста против веб-сайтов и их менеджмента, хотя в некоторых случаях эти атаки также используются для вымогательства. DDoS-атаки могут быть результатом кибершпионажа с целью кражи данных из организации, а не их уничтожения.

17. Усовершенствованные постоянные угрозы (APT)

Усовершенствованная постоянная угроза (Advanced Persistent Threat) – это вид кибератаки, что является точечной, постоянной, изощренной и высоко обеспеченной ресурсами. APT обычно используются для кражи информации у организации с целью получения финансовой выгоды.

Кибератаки типа APT могут продолжаться месяцами или даже годами. Они проникают в сеть, извлекают данные, а затем отфильтровывают их без обнаружения. Типичными целями являются государственные учреждения, университеты, производства, высокотехнологичные отрасли промышленности и сфера обороны.

18. Black Hat SEO

Black Hat SEO – это оптимизация сайта с применением методов, запрещённых поисковыми системами. Она может включать в себя вброс ключевых слов, невидимый текст и маскировку, которые заставляют алгоритм поисковой системы думать, что страница релевантна, когда это не так.

Подобные маркетинговые методы незаконны, поскольку они нарушают основы поиска Google, злоупотребляя системой ранжирования. В результате оптимизаторы Black Hat могут получить штраф или полное удаление своего веб-сайта со страницы результатов поисковой системы (SERP).

2.3. Борьба с киберпреступностью

В настоящее время борьба с киберпреступностью – довольно распространенное явление, ведь кибератаки занимают четвертое место в мире по частоте совершения.

Конечно, спецслужбы не в состоянии полностью контролировать киберпреступность и в связи с этим, число киберпреступлений растет день за днем.

В 2023 году число кибератак в России выросло в три раза, тем самым увеличилось за год на 21 % и достигло 911 тысяч.

Выросло число кибератак на ИТ-компании через шпионское ПО. За год количество зафиксированных атак на государственный сектор составило 403 атаки. По данным МИД РФ: Число кибератак на Россию выросло на 85 %.

Законодательство РФ предусматривает уголовную ответственность за совершение киберпреступлений (Глава 28 УК РФ (статья 272 - 274) лишением свободы сроком от одного до десяти лет и штрафом в размере от 100 тысяч до 500 тысяч рублей. В последние годы, преступления на просторах сети Интернет становятся все более изощренными, исполнители которых хорошо скрываются и поймать их является задачей сложной.

В РФ существует специальный отдел «К», который занимается ловлей киберпреступников, осуществляет борьбу с компьютерными преступлениями и нелегальным оборотом РЭС (радиотехнических средств).

Также хотелось бы сказать об основных правилах компьютерной безопасности:

1. не посещайте сайты, если вы не уверены в их благонадежности и отсутствии на них вирусов;
2. регулярно делайте резервное копирование данных;
3. не устанавливайте программы из непроверенных источников;
4. использование антивирусных программ;
5. не устанавливайте программы из непроверенных источников;

3.1. Практическая часть

Я провел социальный опрос в школе и составил по нему таблицу:

Вопросы	**Учителя**	**Ученики**
Знаете ли вы что такое киберпреступность?	Большинство знают	Большинство знают
У вас когда нибудь воровали деньги в интернет пространстве?	Многие затрудняются ответить	У большинства воровали
Считаете ли вы себя киберграмотным?	Многие затрудняются ответить	Большое большинство считает себя киберграмотным
Какими видами средств пользуетесь чаще всего? Наличные/Безналичные	Наличные деньги	Безналичные деньги
Считаете ли вы киберпреступность	Большинство считают что это является	50/50

актуальной проблемой в наши дни?	проблемой, но на данный момент существуют проблемы важнее	

Заключение

В ходе выполнения проекта на тему: “Киберпреступность”, можно считать, что все поставленные цели и задачи выполнены.

Я определил основные понятия киберпреступности, выявил какие бывают виды, а также выявил методы защиты от кибепреступности.

На сегодняшний день, киберпреступность составляет значительно более серьезную угрозу нежели чем 5-10 лет тому назад, в связи с использованием преступниками новейших информационных технологий, а также через растущую уязвимость современного общества.

Несмотря на все усилия которые государства принимают для борьбы с киберпреступниками, их количеств не уменьшается, а наоборот, растёт. Ни одно государства мира не способно противостоять этому злу самостоятельно. Из всего вышесказанного можно сделать вывод, что чем сильнее становится зависимость жизни общества от компьютерных систем, тем опаснее уязвимость России и в частности других стран от всевозможных киберпреступлений**.** К тому же, хочется отметить, что люди должны как можно чаще напоминать себе о правилах защиты против различных видов киберпреступлений, если каждый человек будет знать хотя бы основные правила защиты перечисленные мною в проекте, то и киберпреступлений в нашей стране будет на порядок меньше.

Список литературы

1. https://translated.turbopages.org/proxy_u/en-ru.ru.1d939f1d-65e73a82-82ea910a-74722d776562/https/en.wikipedia.org/wiki/Cybercrime
2. https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime
3. https://www.cloudav.ru/mediacenter/security/types-of-cybercrime/
4. https://vc.ru/flood/599751-vidy-kiberprestupleniy
5. https://securitymedia.org/info/kiberprestupleniya-vidy-i-sposoby-predotvrashcheniya.html