Оглавление

[Безопасность в интернете 2](#_Toc150359823)

[Противостояние киберпреступникам. Виды киберпреступлений 3](#_Toc150359824)

[Масштабы распространения киберугроз и основные виды киберугроз 5](#_Toc150359825)

[Способы защиты от кибератак: советы по кибербезопасности 7](#_Toc150359826)

# Безопасность в интернете

Способы доступа в Интернет различаются по степени надёжности. Наиболее уязвимым считается выход в Интернет через общие компьютеры или публичные Wi-Fi-сети. Основной риск – кража пароля от аккаунтов в социальных сетях, от почты или электронных кошельков. Поэтому старайтесь не использовать платёжные системы и другие важные сервисы при работе с ненадёжным подключением.

Для шифрования передаваемых через Интернет-данных сайты используют стандарт HTTPS. Шифрование не позволяет сторонним лицам получить доступ к данным, которые вы передаете или принимаете. Это дополнительное средство безопасности. Чтобы воспользоваться им, достаточно в любом браузере перед любым URL ввести [https://](NULL).

Протокол SSL или TLS – это технология, позволяющая обеспечить безопасное подключение по стандарту HTTPS. SSL или TLS использует цифровые ключи шифрования – примерно то же самое, что и обычные ключи. Например, если Вы отправите другу записку, ее сможет прочитать любой, кому она попадет в руки. Однако Вы можете обмениваться записками в парных коробках, ключи от которых есть только у вас и у друга. Если кто-то перехватит Вашу корреспонденцию, ему будет непросто открыть коробку без ключа. Кроме того, если злоумышленник подменит коробку, вы не сможете открыть ее имеющимся ключом и сразу же заподозрите неладное. Протокол SSL или TLS работает по такому же принципу.

Индикаторы безопасности браузера также передают расширенный сертификат подлинности EV (Extended Validation). Сертификаты EV получают сайты, которые одобрены контролирующим органом. Иногда в браузерах индикатор EV отображается в виде названия сайта или регистрирующего органа рядом с адресной строкой. Если Вы сомневаетесь в том или ином сайте, посмотрите, совпадает ли URL в сертификате с URL в браузере – для этого нажмите View Certificate (Посмотреть сертификат).

# Противостояние киберпреступникам. Виды киберпреступлений

Согласно Европейской конвенции по киберпреступности (или преступлениям в киберпространстве) компьютерные преступления можно разделить на четыре типа:

1. Незаконный доступ.
2. Незаконный перехват.
3. Вмешательство в данные.
4. Вмешательство в систему.

Остальные преступления связаны с компьютером или совершаются с помощью компьютера:

1. Преступления, связанные с нарушением авторских прав.
2. Действия, в которых компьютеры используются как орудия преступления (электронные хищения, мошенничества).
3. Преступления, в которых компьютеры играют роль интеллектуальных средств (размещение в сети Интернет детской порнографии, информации, разжигающей национальную, расовую, религиозную вражду).

В 2000 г. на X Конгрессе ООН была принята следующая классификация киберпреступлений. Их разделили на две группы:

1. Насильственные (угроза физической расправы, киберпреследования, детская порнография, кибертерроризм)
2. Ненасильственные (противоправное нарушение владения в киберпространстве, киберворовство, кибермошенничество, реклама услуг проституции в сети Интернет, незаконный оборот наркотиков с использованием сети Интернет, отмывание денег с помощью электронного перемещения, деструктивное киберпреступление)

Кибербезопасность (компьютерная безопасность) – это один из разделов информационной безопасности. Кибербезопасность включает в себя изучение процессов формирования, развития и функционирования различных киберобъектов для выявления возможных источников киберопасности, образующихся при этом. Новые угрозы информационной безопасности характеризуются приставкой «кибер».

Выделяют несколько основных категорий кибербезопасности:

1. Безопасность сетей – действия по защите компьютерных сетей от различных угроз, например, целевых атак или вредоносных программ.
2. Безопасность приложений – защита устройств от угроз, которые преступники могут спрятать в программах. Зараженное приложение может открыть злоумышленнику доступ к данным, которое оно должно защищать. Безопасность приложения обеспечивается еще на стадии разработки, задолго до его появления в открытых источниках.
3. Безопасность информации – обеспечение целостности и приватности данных как во время хранения, так и при передаче.
4. Операционная безопасность – обращение с информационными активами и их защита. К этой категории относится управление разрешениями для доступа к сети или правилами, которые определяют, где и каким образом данные могут храниться и передаваться.
5. Аварийное восстановление – реагирование на инцидент безопасности (действия злоумышленника) и любое другое событие, которое может нарушить работу систем или привести к потере данных. Аварийное восстановление – набор правил, описывающих то, как организация будет восстанавливать рабочие процессы.
6. Повышение осведомленности – обучение пользователей. Это направление позволяет снизить влияние самого непредсказуемого фактора в области кибербезопасности – человеческого. Даже самая защищенная система может подвергнуться атаке из-за чьей-то ошибки или незнания. Каждая организация должна проводить тренинги для сотрудников, школа обучать учеников, рассказывать им о главных правилах, например, не следует открывать подозрительные вложения в электронной почте или подключать сомнительные USB-устройства.

Главная цель системы кибербезопасности – защита информации, как хранящейся, так и передаваемой, предназначенной для обмена. Защита информации – деятельность, направленная на предотвращение утечки информации, несанкционированных и непреднамеренных воздействий на информацию.

# Масштабы распространения киберугроз и основные виды киберугроз

Виды киберугроз

Кибербезопасность борется с тремя видами угроз:

1. Киберпреступления – действия, организованные одним или несколькими злоумышленниками с целью атаковать систему, чтобы нарушить ее работу или извлечь финансовую выгоду.
2. Кибератака – действия, нацеленные на сбор информации, в основном политического характера.
3. Кибертерроризм – действия, направленные на дестабилизацию электронных систем с целью вызвать страх или панику.

Для получения контроля над компьютерными системами злоумышленники используют различные инструменты и приемы:

1. Вирусы – программы, которые заражают файлы вредоносным кодом. Чтобы распространяться внутри системы, они копируют себя сами. Они скрытно проникают в компьютерные системы, и без эффективной защиты бороться с ними невозможно. Вирусы могут нарушить работоспособность компьютеров и программ, уничтожить файлы.
2. Черви – в отличие от вирусов червям для распространения не требуется вмешательства человека: они заражают один компьютер, а затем через компьютерные сети распространяются на другие машины без участия их владельцев.
3. Троянские программы – вредоносы, которые прячутся под маской легального программного обеспечения.
4. Шпионское программное обеспечение – программы, которые втайне следят за действиями пользователя и собирают информацию
5. Программы-вымогатели – шифруют, файлы и данные. Затем преступники требуют выкуп за восстановление и расшифровку, утверждая, что иначе пользователь потеряет данные.
6. Рекламное программное обеспечение – программы рекламного характера, с помощью которых может распространяться вредоносное программное обеспечение. Один из наиболее распространенных типов вредоносных программ. Adware – это программы, которые предназначены для показа рекламы на Вашем компьютере, перенаправления запросов поиска на рекламные вебсайты и сбора маркетинговой информации о Вас, чтобы реклама соответствовала Вашим интересам.
7. Боты – это программы, предназначенные для автоматического выполнения определенных операций. Хакеры могут также пытаться заразить несколько компьютеров одним и тем же ботом, чтобы создать бот-сеть, которая затем будет использоваться для удаленного управления взломанными машинами.
8. Руткиты – позволяют третьей стороне получать удаленный доступ к компьютеру и управлять им. Эти программы используются IT- специалистами для дистанционного устранения сетевых проблем. Но в руках злоумышленников они превращаются в инструмент мошенничества: проникнув на Ваш компьютер, руткиты обеспечивают киберпреступникам возможность получить контроль над ним и похитить Ваши данные или установить другие вредоносные программы. Руткиты умеют качественно маскировать свое присутствие в системе, чтобы оставаться незамеченными как можно дольше. Обнаружение такого вредоносного кода требует ручного мониторинга необычного поведения, а также регулярного внесения корректировок в программное обеспечение и операционную систему для исключения потенциальных маршрутов заражения.
9. Баги – ошибки в фрагментах программного кода. Это не тип вредоносного программного обеспечения, а именно ошибки, допущенные программистом. Они могут иметь пагубные последствия для Вашего компьютера, такие как остановка, сбой или снижение производительности. В то же время баги в системе безопасности – это легкий способ для злоумышленников обойти защиту и заразить Ваше устройство. Обеспечение более эффективного контроля безопасности на стороне разработчика помогает устранить ошибки, но важно также регулярно проводить программные корректировки, направленные на устранение конкретных багов.
10. SQL-инъекция - вид кибератак используется для кражи информации из баз данных. Киберпреступники используют уязвимости в приложениях, управляемых данными, чтобы распространить вредоносный код на языке управления базами данных (SQL)
11. Спам – электронный эквивалент бумажной рекламы, которую обычно бросают в почтовый ящик. Спам в огромных количествах рассылается по электронной почте спамерами и киберпреступниками, целью которых является распространить вредоносный код на компьютерах получателей. Для защиты от спама или совращения количества спама в электронный почтовый ящик целесообразно никогда не отвечать на спам.
12. Фишинг - – вид интернет-мошенничества, представляет собой атаки, цель которых – обманом заполучить конфиденциальную информацию пользователя. Часто в ходе таких атак преступники отправляют жертвам электронные письма, представляясь официальной организацией.
13. Атаки Man-in-the-Middle — Это атака, в ходе которой киберпреступник перехватывает данные во время их передачи – он как бы становится промежуточным звеном в цепи, и жертвы об этом даже не подозревают.
14. DoS-атаки - Киберпреступники создают избыточную нагрузку на сети и серверы объекта атаки, из-за чего система прекращает нормально работать и ею становится невозможно пользоваться. Так злоумышленники, например, могут повредить важные компоненты инфраструктуры и саботировать деятельность организации.
15. Программы-вымогатели – троянские программы, предназначенные для вымогания денег у жертвы. Программы-вымогатели (ransomware) представляют собой тип вредоносного программного обеспечения, используемый киберпреступниками для получения выкупа. Существует два основных типа программ-вымогателей: шифровальщики и блокировщики.

Вредоносный код – это компьютерный код или веб-скрипт, преднамеренно разработанный для создания уязвимостей в системе, с помощью которых он выполняет несанкционированные вредоносные действия, такие как кража информации и данных и другие потенциальные повреждения файлов и вычислительных систем.

# Способы защиты от кибератак: советы по кибербезопасности

Самыми популярными мерами, применяемыми для защиты от киберугроз в мире и в России, являются антивирусная защита, клиентские межсетевые экраны, установка обновлений и резервное копирование данных. Прокомментируем более подробно способы защиты.

1. Обновление программного обеспечения и операционной системы. Использование нового программного обеспечения обеспечивает более надежные системы безопасности.
2. Использование антивирусных программ. Для максимальной безопасности регулярно следует обновлять программное обеспечение.
3. Использование надежных паролей. Не следует применять комбинации, которые легко подобрать или угадать.
4. Нельзя открывать почтовые вложения от неизвестных отправителей. Они могут быть заражены вредоносным программным обеспечением.
5. Нельзя переходить по ссылкам, полученным по почте от неизвестных отправителей или неизвестных веб-сайтов. Это один из стандартных путей распространения вредоносного программного обеспечения. Адрес сайта, на котором Вы вводите платежные данные, должен начинаться с «https», а не с «http». Это значит, что сайт использует протокол защиты информации, который обеспечивает обмен данными исключительно между устройством и сервером.
6. Избегать незащищенных сетей Wi-Fi в общественных местах. В них Вы уязвимы для атак Man-in-the-Middle.

# Понятие о конфиденциальности и персональных данных

Конфиденциальность – это необходимость предотвращения разглашения, утечки какой-либо личной информации.

Персональные данные представляют собой информацию о конкретном человеке. Таких идентифицирующих данных огромное множество, к ним относятся: фамилия, имя, отчество, дата рождения, место рождения, место жительства, номер телефона, адрес электронной почты, фотография, возраст и пр.

Правила защиты персональных данных в сети Интернет:

1. Ограничьте объем информации о себе, находящейся в Интернете. Удалите лишние фотографии, видео, адреса, номера телефонов, дату рождения, сведения о родных и близких и иную личную информацию.
2. Не отправляйте видео и фотографии людям, с которыми Вы познакомились в Интернете и не знаете их в реальной жизни.
3. Отправляя кому-либо свои персональные данные или конфиденциальную информацию, убедитесь в том, что адресат – действительно тот, за кого себя выдает.
4. Используйте только сложные пароли, разные для разных учетных записей и сервисов.
5. Старайтесь периодически менять пароли.
6. Заведите себе два адреса электронной почты – частный, для переписки (приватный и малоизвестный, который вы никогда не публикуете в общедоступных источниках), и публичный – для открытой деятельности (форумов, чатов и так далее).

Вирусы и антивирусные программы

Компьютерные вирусы – одна из самых старых форм вредоносного программного обеспечения. Вирусы самостоятельно копируют себя. Независимо от того, как вирус собирается проявиться его действия, отнимают ресурсы системы. Это замедляет работу компьютера и даже может совсем остановить ее, если вирус потребует слишком много ресурсов или если одновременно будут работать несколько вирусов. Чаще всего компьютерный вирус действует со злым умыслом – либо сам вирус написан как вредоносный, либо проблемы пользователю создают другие вредоносные программы, которые он устанавливает – черви и трояны.

Классификация вирусов:

1. Среда обитания:
   1. Сетевые - распространяются по компьютерным сетям
   2. Файловые – внедряются в файлы с расширением .com, .exe
   3. Загрузочные - внедряются в загрузочный сектор
   4. Файлово – загрузочные
2. Способ заражения
   1. Резидентные – оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение
   2. Нерезидентные – не заражают память компьютера и являются активными ограниченное время операционной системы к объектам заражения и внедряется в них
3. Степень воздействия
   1. Неопасные – не мешают работе компьютера, но уменьшают объем свободной памяти и памяти на дисках
   2. Опасные – могут привести к различным нарушениям в работе компьютера
   3. Очень опасные – приводят к потере программ, уничтожению данных, стиранию информации в системных областях диска
4. Особенности алгоритмов
   1. Паразитические – изменяют содержимое файлов и секторов диска и могут быть легко обнаружены и уничтожены
   2. Репликаторы (черви) - распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии
   3. Невидимки – трудно обнаружить и обезвредить, т. к. они перехватывают обращения ОС к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска
   4. Мутанты – сложно обнаружить, содержат алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют повторяющейся цепочки байтов
   5. Троянские – не способны к самораспространению, но очень опасны, т. к., маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

Для защиты от вирусов следует убедиться, что на всех Ваших устройствах установлена последняя версия антивирусного ПО, которое может активно сканировать Вашу систему и противодействовать вирусам.

Антивирусная программа – это программа, предназначенная для обнаружения, удаления и защиты от компьютерных вирусов. Главной задачей антивируса является предотвращение заражения, еще одна его функция – удаление вредоносного ПО с зараженного компьютера. При использовании антивируса сканирование компьютера на наличие вредоносных программ играет ключевую роль в поддержании безопасности компьютера.

Виды антивирусов:

1. Детекторы - осуществляют поиск характерной для конкретного вируса последовательности байтов в оперативной па-мяти и в файлах и при обнаружении выдают соответствующее сообщение.
2. Ревизоры – запоминают исходное состояние программ, каталогов и системных областей диска до заражения вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние и исходным.
3. Вакцины – резидентные программы, предотвращающие заражение файлов.
4. Доктора - находят зараженные вирусами файлы и «лечат» их, т. е. удаляют из файла тело программы вируса, возвращая файлы в исходное состояние.
5. Фильтры - предназначены для обнаружения подозрительных действий при работе компьютера.

Защита компьютера от вирусов

Работа в Интернете делает компьютер уязвимым для вредоносных программ-вирусов. Чтобы предотвратить заражение, придерживайтесь следующих правил:

1. Регулярно обновляйте браузер, операционную систему и антивирусную базу. Браузер Chrome автоматически обновляется до последней версии при каждом запуске, обеспечивая надёжную защиту без усилий со стороны пользователя.
2. Проверяйте адреса сайтов, не загружайте неизвестные файлы с расширением .exe, .dll, .bat и не переходите по ссылкам из всплывающих окон.
3. Если ваши действия привели к блокировке экрана подозрительным сообщением, закройте браузер в диспетчере задач или мониторе активности своей операционной системы.
4. Загружайте ПО только с официальных сайтов-разработчиков.
5. При неадекватной работе ПО (устройство медленно работает, появляются всплывающие окна, выполняются непонятные платежи) сразу удалите его с помощью последней версии антивирусной программы.
6. Выбирайте зарекомендовавшие себя антивирусные программы и устанавливайте только лицензионные версии.
7. Установите следующие настройки антивирусной программ
   1. включите проактивный и поведенческий анализ – эти режимы позволяют отловить вредоносные программы, которых ещё нет в антивирусной базе;
   2. настройте проверку почтовых сообщений и их вложений;
   3. проводите полное сканирование компьютера и подключаемых устройств не реже 1 раза в неделю.
   4. Не устанавливайте на компьютер сразу несколько средств защиты. Программы распознают друг друга как вредоносное ПО и начинают конкурировать между собой или вообще перестают работать.