**ИНФОРМАЦИОННЫЕ УГРОЗЫ**

В настоящей работе представлены классы, виды, типы информационных угроз, а также меры по их нейтрализации, предотвращению и борьбе с такими угрозами.

## **Анализ информационных угроз. Способы борьбы с ними и меры защиты**

Уровни угроз классифицируют:

### На уровне личности

### На уровне предприятия

### На уровне государства.

# Остановимся подробнее на каждом из них.

### На уровне личности

#### **Компьютерные вирусы**

Существует большое число различных классификаций вирусов. **Основные типы вирусов классифицируют:**

**по среде обитания:**

* **сетевые** вирусы, распространяемые различными компьютерными сетями;
* **файловые** - инфицируют исполняемые файлы, имеющие расширение exe и com. К этому же классу относятся и **макровирусы**, написанные с помощью макрокоманд. Они заражают неисполняемые файлы (в Word, Excel);
* **загрузочные** - внедряются в загрузочный сектор диска или в сектор, содержащий программу загрузки системного диска. Некоторые вирусы записываются в свободные секторы диска, помечая их в FAT-таблице как плохие;
* **загрузочно-файловые** - интегрируют черты последних двух групп;

**по способу заражения (активизации):**

* **резидентные –**при заражении оставляет в оперативной памяти компьютера свою часть, которая потом перехватывает обращения ОС к объектам заражения;
* **нерезидентные –** не заражают оперативную память и проявляют свою активность лишь однократно при запуске инфицированной программы;

**по степени опасности:**

* **не опасные** –не мешают работе компьютера, но могут уменьшать объем свободной памяти (звуковые и видеоэффекты);
* **опасные** - уничтожают часть файлов на диске;
* **очень опасные** - самостоятельно форматируют жесткий диск;

**по особенностям алгоритма:**

* **компаньон-вирусы** не изменяют файлы. Алгоритм их работы состоит в том, что они создают для exe-файлов новые файлы-спутники (дубликаты), имеющие то же имя, но с расширением com. (com-файл обнаруживается первым, а затем вирус запускает exe-файл);
* **паразитические** - при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов (все вирусы кроме компаньонов и червей);
* **черви (репликаторы)** - аналогично компаньонам не изменяют файлы и секторы диска. Они проникают в компьютер по сети, вычисляют сетевые адреса других компьютеров и рассылают по этих адресам свои копии. Черви уменьшают пропускную способность сети, замедляют работу серверов;
* **невидимки (стелс)** - используют набор средств для маскировки своего присутствия в ЭВМ. Их трудно обнаружить, т.к. они перехватывают обращения ОС к пораженным файлам или секторам и подставляют незараженные участки файлов;
* **полиморфики (призраки, мутанты)** - шифруют собственное тело различными способами. Их трудно обнаружить, т.к. их копии практически не содержат полностью совпадающих участков кода;
* **трояны** - маскируется под полезную или интересную программу, выполняя во время своего функционирования еще и разрушительную работу или собирает на компьютере информацию, не подлежащую разглашению. В отличие от вирусов, троянские программы не обладают свойством самовоспроизводства.

**по целостности:**

* **монолитные** - программа представляет единый блок;
* **распределенные** - программа разделена на части. Эти части содержат инструкции, которые указывают как собрать их воедино, чтобы воссоздать вирус.

## **МЕРЫ ПО ЗАЩИТЕ.**

Для того чтобы не подвергнуть компьютер заражению вирусами и обеспечить надежное хранение информации на дисках, необходимо соблюдать следующие правила:

* оснастить компьютер современными антивирусными программами, например NOD32, Doctor Web, и постоянно обновлять их версии перед считыванием с дисков информации, записанной на других компьютерах,
* всегда проверять эти диски на наличие вирусов, запуская антивирусные программы при переносе на компьютер файлов в архивированном виде проверять их сразу же после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами
* периодически проверять на наличие вирусов жесткие диски компьютера, запуская антивирусные программы для тестирования файлов, памяти и системных областей дисков
* обязательно делать архивные копии на дисках ценной информации
* использовать антивирусные программы для входного контроля всех исполняемых файлов, получаемых из компьютерных сетей.

#### **Низкий уровень компьютерной грамотности**

Термин компьютерной грамотности подразумевает под собой умение работать с персональным компьютером, с электронным текстом, электронными таблицами, использовать компьютерные программные средства, создавать презентации и базы данных.

**Уязвимость перед вредоносными программами**

* Пользователи с низкой компьютерной грамотностью часто не знают, как защитить свой компьютер от вирусов, троянов, шпионских программ и других вредоносных программ. Они могут случайно установить опасное ПО, попасть на фишинговые сайты, открыть вредоносную почту или запустить вирус, включенный в электронное письмо.

**Уязвимость перед киберпреступниками**

* Пользователи с низкой компьютерной грамотностью могут быть более подвержены киберпреступникам. Они могут попадаться на уловки мошенников, отвечать на спамовые сообщения, передавать личные данные или финансовые реквизиты, не понимая, что это опасно.

**Потеря данных**

* Пользователи с низкой компьютерной грамотностью могут случайно удалять важные файлы, не знать, как сделать резервную копию данных, не уметь восстанавливать систему после сбоев или вирусных атак. Это может привести к потере документов, фотографий, видео, аудиозаписей и других ценных данных.

**Низкая производительность**

* Пользователи с низкой компьютерной грамотностью могут не знать, как оптимизировать работу своего ПК. Они могут запускать слишком много программ или вкладок в браузере, не удалять временные файлы и кэш, не обновлять драйвера и программное обеспечение, не выполнять дефрагментацию диска и другие меры, которые помогают ускорить работу компьютера.

**Ограниченный доступ к информации и услугам**

* Пользователи с низкой компьютерной грамотностью могут быть ограничены в возможности получать информацию и использовать интернет-услуги. Они могут не знать, как искать нужную информацию, не уметь работать с электронной почтой, облачными сервисами, социальными сетями и другими современными технологиями.

## **МЕРЫ ПО ЗАЩИТЕ.**

Необходимо повышать свою компьютерную грамотность, изучать принципы работы ПК, защиту от вредоносных программ и киберпреступников, уметь выполнять резервное копирование и восстановление данных, оптимизировать работу ПК и использовать современные технологии для получения информации и общения с другими людьми.

Как повысить уровень знаний пользователей ПК.

**Чтение книг и статей о компьютерах**

* Самый простой способ увеличить свои знания о компьютерах и интернете – это чтобы читать книги и статьи на эту тему. Начните с базовых понятий, таких как операционные системы, браузеры, антивирусные программы и т.д.

**Следите за новостями в мире технологий**

* Технологии развиваются очень быстро, и чтобы оставаться в тренде, необходимо всегда быть в курсе новостей в мире технологий. Подписывайтесь на профильные блоги и сайты, читайте новости о новых продуктах, разработках и т.д.

**Участвуйте в обучающих курсах**

* Существует множество обучающих курсов по информационным технологиям, как онлайн, так и офлайн. Рекомендуем присоединиться к одному или нескольким, чтобы получить глубокие знания об информационных технологиях, который могут быть применены на практике.

**Практикуйтесь и экспериментируйте**

* Практикуйтесь и экспериментируйте, чтобы получать больше практического опыта. Научитесь устанавливать программное обеспечение, дополнения для браузеров, проводить диагностику компьютера и т.д. Это поможет вам не только повысить свой уровень знаний, но и получить практические навыки работы.

**Общайтесь с другими экспертами**

* Общайтесь с другими пользователями ПК, которые уже обладают опытом работы с ними. Делитесь своими знаниями и опытом, обсуждайте новые продукты и разработки. Это поможет вам получить новые знания и опыт работы.

#### **Социальная инженерия**

Атаки с использованием социальной инженерии бывают разными. Поэтому важно в целом понимать, что такое [социальная инженерия](https://www.kaspersky.ru/resource-center/definitions/social-engineering) и как она работает. Научившись распознавать основной механизм действия, вы сможете гораздо легче вычислять подобные атаки.

**Ловля «на живца»**

Ловец «на живца» оставляет приманку – например, флешку с вирусом. Нашедший из любопытства вставляет ее в свой компьютер, и вирус поражает систему. Существует даже [флешка, повреждающая компьютеры](https://www.blueapache.com/malicious-usb-drives-found-letterboxes-victoria/), – она заряжается через USB-порт и затем высвобождает мощный заряд через устройство ввода. И стоит такая флешка всего 54 доллара США.

**Претекстинг**

Злоумышленник использует предлог, чтобы привлечь внимание жертвы и заставить ее сообщить информацию. Например, во время безобидного, казалось бы, интернет-опроса у вас могут попросить данные вашего банковского счета. Или к вам подойдет человек с папкой документов и скажет, что проверяет внутренние системы. Но он может оказаться мошенником, пытающимся похитить у вас ценные данные.

**Фишинг**

При фишинговой атаке вы получаете письмо или сообщение от кажущегося надежным источника с просьбой предоставить информацию. Хорошо известный пример – письмо якобы от банка, который просит клиентов «подтвердить» конфиденциальную информацию и направляет их на поддельный сайт, где их учетные данные будут зафиксированы. Целевой фишинг – это отправка письма определенному сотруднику якобы от высшего руководства компании, запрашивающего конфиденциальные сведения.

**Вишинг и смишинг**

Это две разновидности [фишинга](https://www.kaspersky.ru/resource-center/threats/spam-phishing). Первая подразумевает «голосовой фишинг», то есть телефонное мошенничество. Злоумышленник может притвориться сослуживцем – например, сотрудником IT-отдела, которому нужны ваши учетные данные. Вторая – попытка получить данные посредством SMS-сообщений.

**«Ты – мне, я – тебе»**

Говорят, честный обмен – не грабеж, но не в этом случае. Многие социальные инженеры убеждают своих жертв в том, что те получат что-то в обмен на данные или доступ к ним. Так работает фальшивый антивирус, предлагающий пользователю устранить угрозу на его компьютере, хотя сам «антивирус» и есть угроза.

**Взлом электронной почты и рассылка по контактам**

Злоумышленник взламывает почту человека или его учетную запись в социальной сети, получая доступ к его контактам. Теперь от имени жертвы он может сообщить им, что его ограбили, и попросить перечислить ему денег или разослать ссылку на вредоносное ПО или клавиатурный шпион под видом интересного видео.

**«Охота» и фарминг**

И наконец, несколько более продвинутых методов социальной инженерии. Большинство простых методов, описанных выше, являются формой «охоты». Все просто: проникнуть, захватить информацию и убраться восвояси.

Однако некоторые социальные инженеры налаживают связь с жертвой, чтобы получить больше данных за более длительный период времени. Этот метод известен как фарминг и представляет для злоумышленника повышенный риск разоблачения. Но в случае успеха он также дает гораздо больший «урожай».

## **МЕРЫ ПО ЗАЩИТЕ.**

**Как избежать атаки с использованием социальной инженерии**

Социальным инженерам особенно сложно противодействовать, поскольку они используют особенности человеческой натуры – любопытство, уважение к властям, желание помочь другу. Но есть ряд советов о том, как обнаружить их атаки.

**Проверяйте источник**

Задумайтесь на минуту о том, откуда исходит сообщение, – не доверяйте ему слепо. На вашем столе неизвестно откуда появилась флешка? Вам внезапно позвонили и сообщили, что вы получили в наследство 5 миллионов долларов? Ваш руководитель просит в письме предоставить ему массу данных об отдельных сотрудниках? Все это выглядит очень подозрительно, поэтому и действовать следует с осторожностью.

Проверить источник нетрудно. Например, посмотреть на заголовок электронного письма и сравнить его с другими письмами того же отправителя. Проверьте, куда ведут ссылки, – поддельные гиперссылки легко выявить, просто наведя на них курсор (только не нажимайте!). Проверьте орфографию: в банках над перепиской с клиентами работают целые отделы квалифицированных специалистов. Письмо с явными ошибками, вероятно, подделка.

Если сомневаетесь, перейдите на официальный сайт, свяжитесь с представителем и попросите подтвердить или опровергнуть сообщение.

**Что им известно?**

Знает ли тот, кто вам звонит или пишет, всю соответствующую информацию – например, ваше полное имя? Сотрудник банка уж точно должен иметь перед глазами все ваши данные и обязательно спросит проверочное слово, прежде чем разрешит вам вносить изменения в свой счет. Если этого не произошло, с большой долей вероятности письмо, сообщение или звонок – фальшивка. Будьте осторожны!

**Остановитесь и подумайте**

Социальные инженеры часто используют иллюзию срочности в расчете на то, что жертва не будет особо задумываться о происходящем. Всего минута размышлений может помочь вам выявить и предотвратить атаку.

Не спешите сообщать данные по телефону или переходить по ссылке. Лучше перезвоните по официальному номеру или перейдите на официальный сайт. Используйте другой способ связи, чтобы проверить благонадежность источника. Например, если друг в электронном письме просит перечислить ему деньги, напишите или позвоните ему по телефону, чтобы убедиться, что письмо действительно от него.

**Требуйте данные, удостоверяющие личность**

Социальному инженеру проще всего проникнуть в охраняемое здание, неся в руках коробку или кипу папок. Кто-нибудь обязательно придержит для него дверь. Не попадайтесь на эту удочку: всегда требуйте удостоверение личности.

То же правило действует и в других ситуациях. Если у вас запрашивают информацию – уточните имя и номер звонящего или его непосредственного руководителя. Затем просто проверьте эту информацию в интернете или справочнике прежде, чем сообщать какие-либо персональные данные. Если вы не знаете человека, который запрашивает информацию, и все еще сомневаетесь – скажите, что уточните у кого-нибудь и потом перезвоните.

**Используйте надежный спам-фильтр**

Если ваш почтовый клиент недостаточно тщательно фильтрует спам или не помечает письма как подозрительные, попробуйте изменить настройки. Хорошие спам-фильтры используют разнообразную информацию для распознавания нежелательных писем. Они могут выявлять подозрительные файлы или ссылки, заносить в черный список ненадежные IP-адреса или сомнительных отправителей и анализировать содержимое писем, чтобы обнаруживать фальшивки.

**Насколько это правдоподобно?**

Некоторые социальные инженеры рассчитывают на то, что вы не станете вдумываться. Попробуйте оценить, насколько реалистична ситуация, – так вы можете избежать атаки. Например:

* Если бы ваш друг действительно застрял в Китае, он бы вам скорее написал на почту, позвонил или написал SMS?
* Насколько вероятно, что нигерийский принц оставил вам в наследство миллион долларов?
* Стал бы банк по телефону узнавать данные вашего счета? Кстати, многие банки фиксируют все звонки клиентам и всю переписку с ними. Так что, если вы не уверены, – перепроверьте.

**Не спешите**

Будьте особенно осторожны, если вам внушают, что ситуация неотложная. Это стандартный способ злоумышленников помешать вам все обдумать. Если чувствуете, что на вас давят, – притормозите. Скажите, что вам нужно время, чтобы добыть информацию, вам нужно спросить своего начальника, у вас сейчас нет нужных данных, – что угодно, чтобы дать себе время на осмысление.

В большинстве случаев мошенник не станет рисковать, осознав, что эффект неожиданности пропал.

**Защитите свои устройства**

Важно защитить устройства, чтобы даже в случае успешной атаки социальный инженер не смог получить слишком много информации. Будь то смартфон, домашняя сеть или крупная корпоративная система, принцип действия одинаков.

* **Обновляйте защиту от вирусов и вредоносного ПО.** Это поможет предотвратить установку вредоносных программ по ссылкам в фишинговых письмах. Антивирусное ПО, например [Kaspersky Anti-Virus](https://www.kaspersky.ru/antivirus), защитит ваши сети и данные.
* **Регулярно обновляйте ПО и прошивки**, обращая особое внимание на исправления безопасности.
* **Не запускайте смартфон с root-правами, а сеть или компьютер – в режиме администратора.** Даже если социальный инженер получит пароль к вашей учетной записи пользователя, он не сможет изменить конфигурацию системы или что-либо на нее установить.
* **Не используйте один и тот же пароль для разных учетных записей.** Вы ведь не хотите, чтобы злоумышленник, завладев одним паролем, смог войти во все ваши учетные записи.
* **Для самых важных учетных записей используйте двухфакторную аутентификацию**, чтобы их нельзя было взломать с помощью одного лишь пароля. Можно использовать распознавание голоса, дополнительное устройство безопасности, отпечаток пальца или SMS-подтверждение.
* **Если вы только что сообщили пароль от своей учетной записи** и подозреваете, что вас «провели», немедленно смените пароль.
* **Будьте в курсе новых угроз кибербезопасности**– регулярно читайте публикации [нашего Центра ресурсов](https://www.kaspersky.ru/resource-center/), чтобы узнавать о новых методах атаки по мере их появления. Так у вас меньше шансов стать их жертвой.

**Подумайте о своем цифровом следе**

Задумайтесь о вашем присутствии в Сети. Публикуя много личной информации в интернете (например, в социальных сетях), вы помогаете злоумышленникам. Например, в качестве проверочного слова многие сервисы предлагают использовать кличку вашего первого питомца. Делились ли вы этими сведениями в Facebook? Если да, то вы подвергаетесь риску! Кроме того, некоторые социальные инженеры входят в доверие, упоминая недавние события, которыми человек поделился в социальных сетях.

Советуем сдержаннее рассказывать о себе и сделать ваши публикации доступными только для друзей. Не нужно паранойи, просто будьте аккуратны.

Задумайтесь, какими еще аспектами своей жизни вы делитесь онлайн. Если, например, вы разместили в Сети свое резюме, стоит удалить оттуда свой адрес, номер телефона, дату рождения – любую полезную информацию, которой может воспользоваться преступник. Некоторые социальные инженеры очень тщательно готовятся к атаке, собирая все возможные данные о жертве, чтобы поймать ее на крючок. Не давайте им такой возможности.

Атаки с использованием социальной инженерии крайне опасны, поскольку происходят в совершенно обыденных ситуациях. Однако, полностью понимая их механизм и принимая элементарные меры предосторожности, вы гораздо меньше рискуете стать их жертвой.

#### **Разглашение конфиденциальных данных**

**Внутреннее разглашение**

Внутреннее разглашение конфиденциальной информации происходит внутри организации и связано с действиями внутренних сотрудников. Такое разглашение может быть намеренным или случайным. Например, сотрудник может передать информацию третьей стороне из-за личных мотивов или невнимательности.

**Внешнее разглашение**

Внешнее разглашение конфиденциальной информации происходит внутри и вне организации, когда информация передается третьим сторонам или попадает в общедоступные источники. Такое разглашение может осуществляться через утечку данных, взлом систем, физическую кражу документов и другие способы.

**Разглашение в письменной форме**

Разглашение конфиденциальной информации в письменной форме означает передачу данных посредством написания или печати. Этот способ разглашения может быть осуществлен через почтовую пересылку, электронные письма, записки и другие документы.

**Устное разглашение**

Устное разглашение конфиденциальной информации происходит при общении людей в устной форме. Такое разглашение может произойти в ходе разговоров, презентаций, переговоров и других ситуациях, когда информация передается устно.

**Техническое разглашение**

Техническое разглашение конфиденциальной информации связано с использованием специальных технических средств и методов, таких как взлом компьютерных систем, использование компьютерных вирусов или шпионского программного обеспечения для получения доступа к конфиденциальной информации.

**Комбинированное разглашение**

Комбинированное разглашение конфиденциальной информации представляет собой комбинацию различных способов разглашения, например, когда сотрудник организации передает информацию посредством электронных писем и устных указаний.

Прежде чем приступить к борьбе с разглашением конфиденциальной информации, важно разобраться в том, какая из приведенных выше форм разглашения наиболее вероятна для вашей организации. Только после этого вы сможете разработать эффективные меры по предотвращению и пресечению таких случаев.

## **МЕРЫ ПО ЗАЩИТЕ.**

Как предотвратить разглашение?

Разглашение конфиденциальной информации может причинить серьезный ущерб организации или человеку. Чтобы предотвратить разглашение, следует принять ряд мер на различных уровнях:

**Обучение сотрудников:** Организуйте регулярные тренинги и обучения для сотрудников, научите их основам информационной безопасности и значимости сохранения конфиденциальной информации.

Установка политики безопасности: Разработайте и внедрите политику безопасности, в которой определены правила и процедуры для работы с конфиденциальной информацией. Обратите внимание на создание сложных паролей, потребуется двухфакторная аутентификация, ограничение доступа и др.

**Физическая безопасность:** Обеспечьте физическую безопасность помещений, где хранится конфиденциальная информация. Установите системы видеонаблюдения, контроля доступа, ограничьте физический доступ только необходимым сотрудникам.

**Защита информационных систем:** Используйте современные технологии и системы защиты информационных систем. Установите брандмауэры, антивирусы, антишпионы и другие средства защиты. Регулярно обновляйте программное обеспечение и операционные системы.

**Система аудита:** Внедрите систему аудита, которая позволит отслеживать доступ к конфиденциальной информации и контролировать действия сотрудников. Это поможет выявлять и предотвращать возможные проблемы.

**Заключение соглашений о неразглашении:** Включите в трудовые договоры и соглашения с сотрудниками положения о неразглашении конфиденциальной информации.

Использование всех этих мер позволит уменьшить риск разглашения конфиденциальной информации и сохранить ценные данные в безопасности.

**Правовые меры против разглашения**

**Разглашение конфиденциальной информации является нарушением закона.** Для борьбы с такими случаями существуют правовые меры, которые направлены на защиту прав субъектов информации и наказание нарушителей.

**1. Гражданское законодательство**

Гражданское законодательство предоставляет возможность охранять конфиденциальную информацию путем установления договорных обязательств или применения иных мер правовой охраны. Пострадавший от разглашения имеет право обратиться в суд с требованием о защите своих прав и возмещении причиненного ущерба.

**2. Уголовное законодательство**

Уголовное законодательство предусматривает уголовную ответственность за незаконное разглашение конфиденциальной информации. За такие действия могут предусматриваться штрафы, лишение свободы или иные меры пресечения в зависимости от степени нарушения.

**3. Административное законодательство**

Административное законодательство устанавливает административную ответственность за разглашение конфиденциальной информации. Нарушители могут быть оштрафованы или привлечены к другим административным мерам в зависимости от характера нарушения.

**4. Процедуры и регламенты**

В организациях часто разрабатываются внутренние процедуры и регламенты, направленные на предотвращение разглашения конфиденциальной информации. Такие документы могут устанавливать правила использования информации, контроль доступа, наказания за нарушения и другие меры защиты.

**5. Международные соглашения и законы**

Международные соглашения также могут регулировать вопросы разглашения конфиденциальной информации и предусматривать меры защиты. Например, существует ряд соглашений в области защиты интеллектуальной собственности, которые обязывают государства осуществлять контроль и бороться с незаконным разглашением.

В целом, правовые меры против разглашения конфиденциальной информации включают гражданскую, уголовную и административную ответственность, применение внутренних процедур и регламентов, а также соблюдение международных соглашений и законов. Важно соблюдать законодательство и принимать все необходимые меры для предотвращения разглашения и защиты конфиденциальной информации.

#### **Вредоносное ПО**

**Что такое вредоносная программа?**

Термин «вредоносное ПО» – это сокращение термина «вредоносное программное обеспечение», в этом обзоре также называемое вредоносной программой. Вредоносные программы – это программы, намеренно разработанные и внедряемые для нанесения ущерба компьютерам и компьютерным системам. Если работа программы повлекла непреднамеренный ущерб, это обычно называют программной ошибкой.

Чем отличается вирус от вредоносной программы. Разница в том, что вредоносная программа – это общий термин для ряда сетевых угроз, включая вирусы, шпионские программы, рекламные программы, программы-вымогатели и другие типы вредоносных программ. Компьютерный вирус – это один из видов вредоносных программ.

Вредоносные программы могут попасть в сеть в результате фишинга, открытия вредоносных вложений, опасных загрузок, [социальной инженерии](https://www.kaspersky.ru/resource-center/threats/how-to-avoid-social-engineering-attacks) и с переносных накопителей. В этом обзоре рассматриваются распространенные типы вредоносных программ.

**Типы вредоносных программ**

Чтобы защититься от взлома, важно различать атаки различных типов вредоносных программ. Некоторые категории вредоносных программ являются общеизвестными (по крайней мере, по названию), другие – менее известны.

**Рекламные программы**

[Рекламные программы](https://www.kaspersky.ru/resource-center/threats/adware) или программы, существующие за счет демонстрации рекламы, отображают нежелательную, а иногда и вредоносную рекламу на экране устройств, перенаправляют результаты поиска на рекламные сайты и собирают данные пользователей, которые затем можно продать рекламодателям без согласия самих пользователей. Не все рекламные программы являются вредоносным, некоторые из них легальные и безопасны в использовании.

В большинстве случаев пользователи могут влиять на частоту показа рекламных программ и на разрешенные виды загрузок с помощью элементов управления во всплывающих окнах, настроек браузеров, а также, используя блокировщик рекламы.

**Шпионские программы**

[Шпионские программы](https://www.kaspersky.ru/resource-center/threats/how-to-detect-spyware) – это разновидность вредоносных программ, скрывающихся на устройстве, отслеживающих активность и осуществляющих кражу конфиденциальной информации: финансовых данных, учетных записей, данных для входа и прочих данных. Шпионские программы могут распространяться через уязвимости программного обеспечения, быть связны с легальными программами или являться частью троянских программ.

**Программы-вымогатели и программы-шифровальщики**

[Программы-вымогатели](https://www.kaspersky.ru/resource-center/threats/ransomware) – это вредоносные программы, осуществляющие блокировку или отказ доступа пользователей к системе или данным до момента выплаты выкупа. Программы-шифровальщики – это тип программ-вымогателей, выполняющих шифрование пользовательских файлов и требующих оплаты в определенный срок и часто в цифровой валюте, например, в [биткойнах](https://www.kaspersky.ru/resource-center/definitions/what-is-bitcoin). Программы-вымогатели уже много лет представляют угрозу для компаний всех отраслей. По мере того как все больше компаний переходят на цифровые технологии, вероятность стать жертвой атак программ-вымогателей значительно возрастает.

**Троянские программы**

[Троянские программы](https://www.kaspersky.ru/resource-center/threats/trojans) маскируются под легальное программное обеспечение, чтобы обманом заставить пользователей запустить вредоносные программы на компьютере. Поскольку они выглядят достаточно надежными, пользователи загружают их, непреднамеренно заражая свои устройства вредоносными программами. Троянские программы – это, своего рода, точки входа злоумышленников в систему. В отличие от червей, им для работы необходимо устройство. После установки троянской программы на устройство злоумышленники могут использовать ее для удаления, изменения и сбора данных с устройства в рамках ботнета, а также для слежки за устройством и получения доступа к сети.

**Черви**

Черви – это один из наиболее часто встречающихся типов вредоносных программ, распространяющихся по компьютерным сетям, используя уязвимости операционной системы. Черви представляют собой отдельные программы, распространяющиеся путем самокопирования с целью заражения других компьютеров, при этом никаких действий со стороны пользователей или злоумышленников не требуется. Благодаря способности быстро распространяться, черви часто используются для выполнения фрагментов кода, созданного для повреждения системы, например, они могут удалять файлы в системе, шифровать данные для атаки программы-вымогателя, красть информацию и создавать ботнеты.

**Вирусы**

Вирус – это фрагмент кода, который вставляется в приложение и запускается при его запуске. Попав в сеть, вирус может использоваться для кражи конфиденциальных данных, запуска DDoS-атак или атак программ-вымогателей. Обычно вирус распространяется через зараженные веб-сайты, при совместном доступе к файлам, при загрузке зараженных вложений электронной почты. Вирус бездействует до момента активации зараженного файла или программы. После этого вирус начинает распространяться в системе.

**Клавиатурные шпионы**

[Клавиатурные шпионы](https://www.kaspersky.ru/resource-center/definitions/keylogger) – это разновидность шпионских программ, отслеживающих активность пользователей. Они могут использоваться в законных целях, например, родители могут с их помощью контролировать действия детей в интернете, а компании отслеживать активность сотрудников. Однако злоумышленники могут использовать клавиатурные шпионы для кражи паролей, банковских данных и прочей конфиденциальной информации. Клавиатурные шпионы могут попасть систему в результате фишинга, социальной инженерии или вредоносных загрузок.

**Боты и ботнеты**

Бот – это компьютер, зараженный вредоносной программой, которым злоумышленники могут управлять удаленно. Боты, иногда называемые зомби-компьютерами, могут использоваться для запуска атак, а также стать частью [ботнета](https://www.kaspersky.ru/resource-center/threats/botnet-attacks) – набора ботов, объединенных в сеть. Ботнеты могут включать миллионы устройств, как правило, они распространяются незаметно. Ботнеты позволяют злоумышленникам совершать различные вредоносные действия: DDoS-атаки, рассылку [спама и фишинговых сообщений](https://www.kaspersky.ru/resource-center/threats/spam-phishing), а также распространять другие типы вредоносных программ.

**Потенциально нежелательные программы**

Потенциально нежелательные программы (ПНП) – это программы, которые могут включать рекламу, панели инструментов и всплывающие окна, не имеющие отношения к самой загруженной программе. Строго говоря, ПНП не всегда являются вредоносными. Разработчики ПНП отмечают, что, в отличие от вредоносных программ, ПНП загружаются пользователями добровольно. Однако известно, что пользователи, в основном, загружают ПНП неосознанно или по невнимательности.

ПНП часто поставляются в комплекте с другими легальными программами. Большинство людей загружают ПНП, поскольку не прочитали мелкий шрифт при установке новой программы и не осознали, что выбирали также установку дополнительных не требуемых для их целей программ.

**Гибридные вредоносные программы**

Большинство современных вредоносных программ представляет собой комбинацию различных типов, часто включая элементы троянских программ, червей, а иногда и вирусов. Часто вредоносные программы сначала выглядят как троянские, но после запуска распространяются по сети как черви.

**Бесфайловые вредоносные программы**

Бесфайловые вредоносные программы используют легальные программы для заражения компьютера. Они не используют файлы и не оставляют следов, что затрудняет их обнаружение и удаление. В основных типах атак бесфайловые вредоносные программы начали применяться в 2017 году, однако многие из них существуют уже давно.

Бесфайловые программы не хранятся в файлах и не устанавливаются на устройство, они попадают непосредственно в память, а вредоносный контент никогда не затрагивает жесткий диск. Киберпреступники все чаще используют бесфайловые вредоносные программы. Они позволяют осуществлять эффективные атаки, поскольку их обнаружение традиционными антивирусами затрудняется вследствие небольшого размера и отсутствия файлов для проверки.

**Логические бомбы**

Логические бомбы – это тип вредоносных программ, которые активируются только при определенном условии, например, в определенную дату и время или при 20-м входе в учетную запись. Вирусы и черви часто содержат логические бомбы для исполнения вредоносного кода в заранее определенное время или при выполнении определенного условия. Ущерб, причиняемый логическими бомбами, варьируется от изменения всего нескольких байтов данных до запрета на чтение жестких дисков.

## **МЕРЫ ПО ЗАЩИТЕ.**

**Методы защиты от вредоносного программного обеспечения**

**Установка антивирусного программного обеспечения**

Одним из основных методов защиты от вредоносного программного обеспечения является установка и регулярное обновление антивирусного программного обеспечения. Антивирусные программы сканируют систему на наличие вредоносных программ и блокируют их действие. Они также могут предупреждать о потенциально опасных сайтах и файловых вложениях.

**Обновление программ и операционной системы**

Вредоносное программное обеспечение может использовать уязвимости в программном обеспечении и операционной системе для проникновения в систему. Поэтому важно регулярно обновлять все программы и операционную систему до последних версий, чтобы исправить известные уязвимости и улучшить безопасность системы.

**Осторожность при открытии вложений в электронной почте и скачивании файлов**

Вредоносное программное обеспечение может быть распространено через вредоносные вложения в электронной почте или ненадежные файлы, загружаемые из интернета. Поэтому необходимо быть осторожным при открытии вложений в электронной почте, особенно если они пришли от незнакомого отправителя. Также следует избегать скачивания файлов с ненадежных и непроверенных источников.

**Регулярное создание резервных копий данных**

В случае атаки вредоносного программного обеспечения, может потребоваться восстановление данных. Поэтому регулярное создание резервных копий данных является важным методом защиты. Резервные копии могут быть созданы на внешних носителях, в облачном хранилище или на других компьютерах.

**Использование брандмауэра**

Брандмауэр – это программное или аппаратное устройство, которое контролирует и фильтрует сетевой трафик, блокируя нежелательные соединения и защищая систему от внешних атак. Включение и настройка брандмауэра может помочь предотвратить проникновение вредоносного программного обеспечения.

**Осторожность при посещении веб-сайтов**

Вредоносное программное обеспечение может быть распространено через вредоносные веб-сайты. Поэтому следует быть осторожным при посещении веб-сайтов, особенно если они выглядят подозрительно или предлагают скачать ненадежное программное обеспечение. Также рекомендуется использовать надежные браузеры и включить функцию блокировки вредоносных сайтов.

Это лишь некоторые из методов защиты от вредоносного программного обеспечения. Важно помнить, что безопасность системы требует постоянного внимания и актуальных знаний о новых угрозах и методах защиты.

#### **Хищение информации**

**Кража данных: определение**

Кража данных, также называемая хищение информации – это незаконная передача или хранение личной, конфиденциальной и финансовой информации: паролей, программных кодов и алгоритмов, а также авторских процессов и технологий. Кража данных считается серьезным нарушением безопасности и конфиденциальности с потенциально неблагоприятными последствиями как для частных лиц, так и для организаций.

**Классификация и способы кражи данных.**

Все хищения данных осуществляются либо перехватом сообщений на линиях связи, либо через воровство носителя информации. Основные сценарии описаны далее.

**Кража физического носителя** Самый прямой и грубый способ. Большинство современных устройств — ноутбуки, смартфоны, планшеты, подключаемые внешние диски и флешки — достаточно малы, чтобы можно было украсть их мимоходом, пройдя рядом со столом, где они лежат (например, если владелец отлучился на минуту от рабочего места). У крупных компьютеров можно похитить жесткие диски, причем не обязательно безвозвратно. Весьма легко вообразить злоумышленника, который извлечет диск после окончания рабочего дня, скопирует всю интересующую его информацию и вернет накопитель на место ранним утром следующего дня. В таком сценарии владелец устройства даже не догадается о несанкционированном доступе к его данным.

**Кража при доступе к носителю** При наличии физического доступа к носителю можно просто поработать на компьютере в отсутствие хозяина. Обеденный перерыв, длительные совещания, время после ухода по окончании рабочего дня — у коллеги-злоумышленника есть немало способов посидеть за чужой клавиатурой. Если пароль учетной записи слаб или вообще отсутствует, то украсть данные сумеет любой, кто работает рядом. Впрочем, даже очень хороший пароль не всегда спасает: в конце концов, сотрудник может открыто попросить разрешения воспользоваться устройством, сославшись на неисправность собственного компьютера и необходимость срочно отправить письмо или файл. Далее, например, к машине подключается флешка с вредоносной программой, скачивающей данные. К этой же категории относится возможность подсмотреть информацию. Распространены случаи, когда множество сотрудников работает в одном большом помещении без перегородок, и соседям хорошо видно, кто что делает. Соответственно, преступник может как наблюдать лично, так и установить небольшую камеру, которая запишет все, что выводилось на экран чужого монитора.

**Удаленная кража по сети** Если машина подключена к проводной или беспроводной сети, то прямой физический доступ к ней необязателен. В интернете доступно множество вирусов, троянских программ, бекдоров и прочих вредоносных агентов, которые злоумышленник может внедрить разными способами (скажем, путем эксплуатации уязвимостей). Также данные могут быть перехвачены при помощи снифферов, если каналы связи плохо защищены.

**Кража данных с внешних серверов** Наконец, если данные хранятся в интернете (в облачном хранилище, на почтовом сервере и т.п.), то преступники могут осуществить несанкционированный доступ к этим ресурсам. Для пользователей такой сценарий опасен тем, что помимо установки хорошего пароля у них нет никакой другой возможности повлиять на сохранность информации — всё программное обеспечение и все настройки доступа осуществляет владелец сервиса.

## **МЕРЫ ПО ЗАЩИТЕ.**

Большинство краж обусловлены не хитроумными планами злоумышленников, а беспечностью пользователей. Не оставляйте без присмотра флешку и смартфон, защищайте сложным паролем ноутбук и компьютер, выходите из системы, даже отлучаясь лишь на пару минут — и вероятность успеха преступников заметно снизится. Особую сложность проблема хищения данных представляет в крупных компаниях. Сотрудники сидят в одном большом зале, каждому видно происходящее на мониторах коллег, и к тому же в помещение могут заходить клиенты либо соседи по офисному комплексу. Информация кочует с компьютера на компьютер на десятках флешек, а практика использования чужих машин является нормой. Иногда существует несколько стандартных логинов и паролей, которые знают все. В таких условиях утечки неизбежны. В идеальной ситуации каждое рабочее место должно быть огорожено. Если такой возможности нет, отдельные ячейки должны получить хотя бы те машины, где обрабатывается важная и конфиденциальная информация. Не должно быть никаких общих, универсальных аккаунтов и кодов доступа: для каждого сотрудника — персональный логин и пароль. Учетные данные должен выдавать администратор, во избежание появления простых и примитивных комбинаций. Нужно также следить за тем, чтобы на рабочем месте не было стикеров с паролями. Если сотрудник неспособен запомнить пароль, то пусть он хотя бы носит записку с ним в бумажнике: сохранности кошелька должное внимание уделяют все люди. Желательно приучить всех работников к мысли, что если они разрешают коллеге временно поработать на своей машине, то им лучше выйти из системы: пусть сотрудник входит под своим именем. Это позволяет избежать получения чужих прав доступа и отследить, кто проявляет подозрительную активность. Важные и конфиденциальные данные на серверах должны быть защищены паролем; желательно, чтобы их видели только те, кому разрешен доступ к ним. Впрочем, разрабатывая правила защиты информации, нельзя чрезмерно усердствовать. Если данные о закупках туалетной бумаги засекречены подобно устройству ядерной бомбы, сотрудники начинают воспринимать такие меры не как политику информационной безопасности, а как самодурство начальников — и, следовательно, нарушать правила везде, где нет прямого надзора. Также важно учесть, что любое усиление защиты данных имеет свою цену — как прямую (стоимость программных и аппаратных продуктов), так и косвенную (усложнение работы, снижение производительности). Поэтому комплекс мер по защите информации следует разрабатывать соизмеряя затраты с возможным ущербом от утечки данных.

### На уровне предприятия

#### **Промышленный шпионаж**

**Промышленный шпионаж** - форма недобросовестной конкуренции, при которой осуществляется незаконное получение, использование, разглашение информации, составляющей коммерческую, служебную или иную охраняемую законом тайну с целью получения преимуществ при осуществлении предпринимательской деятельности, а также получения материальной выгоды. Целью промышленного шпионажа является получение данных о перспективах деятельности конкурента, производственных процессах, торговой стратегии и результаты научных исследований и промышленных разработок, об организации, продающие его товар, списков потребителей, расчетных документов.

**Классификация Промышленного шпионажа.**

1. **Кража коммерческой тайны**

Кража коммерческой тайны — один из самых распространенных видов промышленного шпионажа, который несет значительные убытки для компаний. Конфиденциальная информация и интеллектуальная собственность, такие как ноу-хау, собственные разработки могут быть украдены конкурентами с целью получения преимущества на рынке.

Кража коммерческой тайны может подразумевать передачу в чужие руки:

* технической документации;
* чертежей;
* сведений об организации производства;
* любой другой конфиденциальной информации, которую компания считает ценной и повышающей свою конкурентоспособность.

Украденная информация может быть использована самыми разнообразными способами: от производства поддельной продукции до создания более эффективного производства и устранения конкурентов в целом.

Охрана коммерческой тайны — это обязанность, которую несет каждый сотрудник компании. Организации должны строго контролировать доступ к конфиденциальной информации, обучать сотрудников политике безопасности и проводить необходимые проверки кандидатов на трудоустройство. Тем не менее, несмотря на все меры предосторожности, кража ценных данных все равно происходят регулярно. Но сокращать вероятность этого — обязанность руководства и службы безопасности любой компании.

1. **Кибератаки и хакинг**

На данный момент кибератаки и хакинг стали неотъемлемой частью операции по получению доступа к чужой конфиденциальной информации. Даже более — кибершпионаж стал наиболее популярным и одним из самых эффективных методов добычи технологий. Развитие информационных технологий и перемещение все больших массивов данных в цифровой вид делает ставку на кибершпионаж вполне оправданной. При этом в ход идет не только прямая кража данных посредством взлома информационных систем и поиска их уязвимостей. Методы социальной инженерии могут заставить ничего не подозревающего сотрудника компании, имеющего доступ к конфиденциальной информации, предоставить эти данные в распоряжение третьих лиц.

Одним из самых известных подобных случаев промышленного шпионажа стала операция «Ночной дракон» 2011 года. Тогда, по утверждению компании-производителя антивирусных программ McAfee, китайские хакеры смогли взломать системы крупнейших американских нефтяных компаний, при этом сама утечка длилась в течение нескольких лет — как минимум, с 2009 года. Сами компании при этом названы не были. Впрочем, ExxonMobil, Chevron и ConocoPhillips в прямом запросе эту информацию не подтвердили, но в то же время и не опровергли.

1. **Покупка или продажа информации**

Одним из методов ведения промышленного шпионажа является покупка конфиденциальной информации. Этот метод активно используется как правительственными агентствами, так и промышленными корпорациями.

Как показывает практика, от подобных случаев не застрахованы даже всемирно известные корпорации. Широко известным стало дело 2018 года, когда в США буквально на стойке регистрации аэропорта арестовали бывшего инженера компании Apple Сяолан Чжена, собирающегося вылететь в Китай. В 2022 году его признали виновным в продаже коммерческих секретов IT-гиганта. Речь шла о продаже схем и чертежей центрального процессора проекта беспилотного автомобиля Apple Car. В деле фигурирует китайский производитель автомобилей Xiaopeng Motors, который, тем не менее, официально сообщил о том, что со всем уважением относится к законодательству по защите прав на интеллектуальную собственность.

## **МЕРЫ ПО ЗАЩИТЕ.**

**Как защитить компанию от промышленного шпионажа?**

* Создать четкий и понятный регламент работы с важной информацией. Обработка, хранение, передача такой информации должны осуществляется по отработанной схеме и строгим правилам для исключения утечек и нецелевого использования.
* Ограничить доступ к информации. Оптимальное решение – система доступа с минимальными привилегиями, выделение ограниченного круга лиц, которые располагают правом распоряжения данными.
* Обучить персонал правилам работы с [конфиденциальными сведениями](https://rt-solar.ru/products/solar_dozor/blog/2752/), основам кибербезопасности. Подписать соглашение о неразглашении коммерческой тайны, проинструктировать об ответственности за нарушение законодательства в сфере защиты информации.
* Проводить эффективную кадровую политику в организации. Вести продуманный отбор кадров с учетом проверки послужного списка кандидата, его репутации. При подборе сотрудников уделять повышенное внимание на управляющие должности, использовать средства технической проверки надежности персонала вроде полиграфа.
* Позаботиться о создании на предприятии службы безопасности и ведении регулярного мониторинга информационной безопасности. Отслеживать инциденты безопасности, собирать, анализировать информацию по ним, принимать превентивные меры.
* Использовать СЗИ согласно уровню критичности информации и другие дополнительные технические меры, направленные на создание безопасного информационного периметра организации, с тщательным контролем всех происходящих событий и сбором статистических данных.

Защита от промышленного шпионажа потребует проведения комплекса организационно-правовых и технических мер. Немаловажным фактором здесь является своевременное выявление и предотвращение утечек конфиденциальных данных. В качестве инструмента предотвращения шпионской детальности можно использовать [Solar Dozor](https://rt-solar.ru/products/solar_dozor/). С его помощью возможно заблокировать передачу конфиденциальных сведений, выявить следы корпоративного мошенничества, провести мероприятия по профилактике инцидентов информационной и экономической безопасности.

**Защита от Кибератаки и хакинга**

Для защиты от подобного рода атак компаниям необходимо разрабатывать соответствующие меры в области кибербезопасности:

* использование надежных алгоритмов шифрования;
* распределение прав доступа;
* постоянное обновление информационных систем в соответствии с последними стандартами безопасности;
* информирование сотрудников о возможных рисках и угрозах

— все это является важными превентивными мерами в борьбе с киберпреступностью и промышленным шпионажем.

Защита коммерческой тайны является важным элементом бизнес-стратегии любой компании. Предотвращение утечки информации может быть достигнуто путем:

* контроля доступа сотрудников к конфиденциальной информации;
* установления мер безопасности на рабочих местах;
* разработки действенной и эффективной политики безопасности.

Важно обучать сотрудников правилам безопасности и контролировать их действия в рамках рабочих обязанностей. Денежные штрафы или увольнение сотрудников, нарушающих политику безопасности, могут также служить мерой защиты от утечки конфиденциальной информации.

#### **Искажение/Уничтожение информации**

### Непосредственное воздействие на носители защищаемой информации.

### Вывод из строя технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи.

### Нарушение режима работы перечисленных средств и технологии обработки информации.

### Вывод из строя и нарушение режима работы систем обеспечения функционирования названных средств.

Способами нарушения режима работы технических средств отображения, хранения, обработки, воспроизведения, передача информации, средств связи и технологии обработки информации, приводящими к уничтожению, искажению и блокированию информации, могут быть:

* повреждение отдельных элементов средств;
* нарушение правил эксплуатации средств;
* внесение изменений в порядок обработки информации;
* заражение программ обработки информации вредоносными программами;
* выдача неправильных программных команд;
* превышение расчетного числа запросов;
* создание помех в радио эфире с помощью дополнительного звукового или шумового фона, изменения (наложения) частот передачи информации;
* передача ложных сигналов – подключение подавляющих фильтров в информационные цепи, цепи питания и заземления;
* нарушение (изменение) режима работы систем обеспечения функционирования средств.

К видам дестабилизирующего воздействия на защищаемую информацию со стороны технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи и систем обеспечения их функционирования относятся выход средств из строя; сбои в работе средств и создание электромагнитных излучений

При намеренной дезинформации применяют как заведомую ложь, так и полуправду, создающие искаженное представление о событиях. Наиболее распространенные приемы дезинформации:

* прямое сокрытие фактов;
* тенденциозный подбор данных
* нарушение логических и временных связей между событиями;
* подача правды в таком контексте (добавлением ложного факта или намека), чтобы она воспринималась как ложь;
* изложение важнейших данных на ярком фоне отвлекающих внимание сведений
* смешивание разнородных мнений и фактов;
* изложение данных словами, которые можно истолковывать по-разному;
* отсутствие упоминания ключевых деталей факта.

В процессе сбора и получения информации могут возникнуть искажения. Основные причины искажений информации:

· передача только части сообщения;

· интерпретация услышанного в соответствии со своими знаниями и представлениями;

· пропуск фактуры через призму субъективно-личностных отношений.

## **МЕРЫ ПО ЗАЩИТЕ.**

**Технологии защиты** данных основываются на применении современных **методов**, которые предотвращают утечку информации и ее потерю.

Сегодня используется шесть основных способов защиты:

# Препятствие;

# Маскировка;

# Регламентация;

# Управление;

# Принуждение;

# Побуждение.

Все перечисленные методы нацелены на построение эффективной технологии защиты информации, при которой исключены потери по причине халатности и успешно отражаются разные виды угроз.

Под препятствием понимается способ физической защиты информационных систем, благодаря которому злоумышленники не имеют возможность попасть на охраняемую территорию.

Маскировка – способы защиты информации, предусматривающие преобразование данных в форму, не пригодную для восприятия посторонними лицами. Для расшифровки требуется знание принципа. Управление – способы защиты информации, при которых осуществляется управление над всеми компонентами информационной системы.

Регламентация – важнейший метод защиты информационных систем, предполагающий введение особых инструкций, согласно которым должны осуществляться все манипуляции с охраняемыми данными.

Принуждение – методы защиты информации, тесно связанные с регламентацией, предполагающие введение комплекса мер, при которых работники вынуждены выполнять установленные правила.

Если используются способы воздействия на работников, при которых они выполняют инструкции по этическим и личностным соображениям, то речь идет о побуждении.

**Способы защиты** информации предполагают использование определенного **набора средств**. Для предотвращения потери и утечки секретных сведений используются следующие средства:

# Физические;

# Программные и аппаратные;

# Организационные;

# Законодательные;

# Психологические.

Физические средства защиты информации предотвращают доступ посторонних лиц на охраняемую территорию. Основным и наиболее старым средством физического препятствия является установка прочных дверей, надежных замков, решеток на окна. Для усиления защиты информации используются пропускные пункты, на которых контроль доступа осуществляют люди (охранники) или специальные системы. С целью предотвращения потерь информации также целесообразна установка противопожарной системы. Физические средства используются для охраны данных как на бумажных, так и на электронных носителях.

Программные и аппаратные средства – незаменимый компонент для обеспечения безопасности современных информационных систем. Аппаратные средства представлены устройствами, которые встраиваются в аппаратуру для обработки информации. Программные средства – программы, отражающие хакерские атаки. Также к программным средствам можно отнести программные комплексы, выполняющие восстановление утраченных сведений. При помощи комплекса аппаратуры и программ обеспечивается резервное копирование информации – для предотвращения потерь.

Организационные средства сопряжены с несколькими методами защиты: регламентацией, управлением, принуждением. К организационным средствам относится разработка должностных инструкций, беседы с работниками, комплекс мер наказания и поощрения. При эффективном использовании организационных средств работники предприятия хорошо осведомлены о технологии работы с охраняемыми сведениями, четко выполняют свои обязанности и несут ответственность за предоставление недостоверной информации, утечку или потерю данных.

Законодательные средства – комплекс нормативно-правовых актов, регулирующих деятельность людей, имеющих доступ к охраняемым сведениям и определяющих меру ответственности за утрату или кражу секретной информации.

Психологические средства – комплекс мер для создания личной заинтересованности работников в сохранности и подлинности информации. Для создания личной заинтересованности персонала руководители используют разные виды поощрений. К психологическим средствам относится и построение корпоративной культуры, при которой каждый работник чувствует себя важной частью системы и заинтересован в успехе предприятия.

**Защита передаваемых электронных данных**. Для обеспечения безопасности информационных систем сегодня активно используются методы шифрования и защиты электронных документов. Данные технологии позволяют осуществлять удаленную передачу данных и удаленное подтверждение подлинности.

Методы защиты информации путем шифрования (криптографические) основаны на изменении информации с помощью секретных ключей особого вида. В основе технологии криптографии электронных данных – алгоритмы преобразования, методы замены, алгебра матриц. Стойкость шифрования зависит от того, насколько сложным был алгоритм преобразования. Зашифрованные сведения надежно защищены от любых угроз, кроме физических.

Электронная цифровая подпись (ЭЦП) – параметр электронного документа, служащий для подтверждения его подлинности. Электронная цифровая подпись заменяет подпись должностного лица на бумажном документе и имеет ту же юридическую силу. ЭЦП служит для идентификации ее владельца и для подтверждения отсутствия несанкционированных преобразований. Использование ЭЦП обеспечивает не только защиту информации, но также способствует удешевлению технологии документооборота, снижает время движения документов при оформлении отчетов.

Для успешности борьбы с вероятной дезинформацией следует:

# различать факты и мнения;

# применять дублирующие каналы информации;

# исключать все лишние промежуточные звенья и т. п.

#### **Недобросовестная конкуренция (дезинформация о конкуренте, разглашение конфиденциальных данных руководителя)**

Недобросовестная конкуренция – это форма соперничества между участниками рынка, которая нарушает правила закона и этики деловых отношений. Такие техники охватывают широкий спектр стратегий и могут нанести значительный вред бизнесу и репутации компании.

### Разглашение коммерческой тайны, то есть незаконное распространение информации, охраняемой законом, о составляющей конкурентной преимущества предприятия.

### Приобретение результатов чужих работ или деятельности путем использования коммерческой тайны или иной информации без согласия правообладателя. Это может привести к укреплению позиций недобросовестного конкурента и дискредитации оригинального создателя продукта или услуги.

### Использование ложных сведений для индивидуализации товаров или услуг конкурентов. Такое использование может привести к заблуждению потребителей и подорвать доверие к брендам или торговым маркам, которые основываются на качестве и надежности.

Кроме того, в рамках недобросовестной конкуренции используются различные средства для получения конфиденциальной информации или интеллектуальной собственности. Например, это может быть уклонение от закона о защите персональных данных или нарушение юридического регулирования в области информационной безопасности.

Таким образом, недобросовестная конкуренция представляет серьезную угрозу для предприятий, которые стремятся соблюдать правила честной и открытой конкуренции. Для предотвращения подобных практик необходимо соблюдать законодательство, укреплять интеллектуальную собственность и информационную безопасность, а также осуществлять надлежащий контроль и наказание за нарушения.

### Использование результатов интеллектуальной деятельности представляет собой один из типов недобросовестной конкуренции. В данном случае речь идет о неправомерном использовании (распространении, приобретении, получении) информации или результатов интеллектуальной деятельности, которые защищены законом об охране интеллектуальной собственности.

К такому использованию можно отнести: незаконное разглашение тайны коммерческой, индивидуализации или иную охраняемую законом информацию или результаты интеллектуальной деятельности, создание и распространение неточных или искаженных сведений о товарах, услугах или лицах, дискредитация конкурента с помощью ложных или искаженных сведений.

Такое использование интеллектуальной деятельности может причинить серьезный вред бизнесу или репутации компании. Поэтому, важно знать свои права и обеспечивать их защиту.

В случае недобросовестной конкуренции, связанной с использованием результатов интеллектуальной деятельности, можно применять юридические меры, предусмотренные законодательством. Например, подать иск в суд для защиты прав на интеллектуальную собственность, требовать компенсации за причиненный ущерб или возмещение морального вреда.

Недобросовестные методы конкуренции, включая использование результатов интеллектуальной деятельности, создают негативные последствия для бизнеса и общества в целом. Поэтому, важно соблюдать нормы законодательства и честно конкурировать на рынке товаров и услуг.

### Дискредитация представляет собой один из типов недобросовестной конкуренции, которая направлена на нанесение ущерба репутации и доверию к юридическим и коммерческим субъектам.

Одним из способов дискредитации является распространение ложных, неточных или искаженных сведений о деятельности конкурентов. При этом основными объектами атаки могут быть результаты творческой или интеллектуальной деятельности, товары, услуги или работы, охраняемые законом или имеющие признаки индивидуализации.

В качестве результата дискредитации конкурент может получить преимущество в условиях рыночной конкуренции, причинив ущерб репутации или доходам других субъектов.

## **МЕРЫ ПО ЗАЩИТЕ.**

Дискредитация

Законодательство предусматривает ответственность за дискредитацию, включая возможность требования компенсации морального и материального вреда, возмещение убытков и применение иных санкций к лицам, распространяющим ложные или искаженные сведения.

В общем, целях защиты собственных интересов и предотвращения недобросовестной конкуренции, юридическим лицам рекомендуется регистрировать свои средства индивидуализации и обеспечивать их надлежащую охрану. Такая защита позволяет владельцу исключительного права использовать и распространять свои товары и услуги под уникальными знаками и идентификационными средствами, а также более эффективно бороться с нарушителями и признаками недобросовестной конкуренции.

#### **Человеческий фактор**

### Неосведомленность об угрозе

Под удар киберпреступников могут попасть не только крупные компании. Большинство атак не является целевыми, злоумышленники часто просто сканируют сеть в поисках потенциальных целей для взлома или, например, рассылают электронные письма с вредоносными вложениями. Небольшие компании часто не слишком заботятся о защите своей цифровой среды, причем это касается не только сотрудников, но и руководителей. Да, на компьютерах может быть установлен коммерческий антивирус, потому что «так надо». При этом сервер сети будет стоять где-нибудь на складе в свободном доступе. Никаких регламентов или правил поведения в части информационной безопасности для сотрудников не существует. Плюс к этому — отсутствие выстроенной системы доступа, информирования сотрудников об угрозах и четкого плана реагирования на компьютерные инциденты. Такой подход встречается до сих пор, и его сложно объяснить чем-то еще, кроме неосведомленности об угрозе и последствиях случайной атаки.

### Отсутствие понимания ценности данных

Это чаще всего касается тех сотрудников, которые должным образом не проинструктированы и не вовлечены в процесс защиты данных в компании. Разобщенность в этом вопросе — краеугольный камень уязвимости всей сетевой инфраструктуры. К сожалению, недостаточно использовать современное ПО и грамотно настроенную сеть, если сотрудники не будут осознавать ценность информации, с которой они работают. В этом случае злоумышленникам гораздо проще зайти в сеть, применив методы социальной инженерии, чем искать программные бреши в обороне. И чем хуже выстроена защита в компании, тем выше риск возникновения инцидента, началом которого может стать запуск на рабочем компьютере неизвестной флешки или вложения из «письма счастья».

### Отсутствие тренингов для персонала

В компании может быть выстроена защитная инфраструктура, а также работать собственный отдел по информационной безопасности. Но также важно, чтобы сотрудники знали, как вести себя, чтобы предупредить возникновение угроз. Для этого бывает недостаточно наличия одних только регламентов и правил, которые на практике часто существуют только на бумаге. Ведь чаще всего сотрудник концентрируется лишь на выполнении повседневных задач и редко задумывается о цифровой гигиене. Даже подкованные технические специалисты могут не знать, как предупреждать инциденты или правильно реагировать на них. Соответствующие тренинги с периодической проверкой знаний не только закрепляют безопасное поведение, но и повышают общую культуру цифровой безопасности.

### Намеренное причинение ущерба

К сожалению, такие случаи тоже нередки. Самая серьезная уязвимость системы — злоумышленник внутри. В этом случае ущерб напрямую зависит от того, какими полномочиями наделен сотрудник на момент совершения атаки. Отдельно стоит выделить уязвимость физического доступа, когда человек имеет прямой доступ к объекту атаки — например, к важному серверу. В этом случае у злоумышленника появляется практически полная свобода действий — от мелкого вредительства до полного уничтожения данных. Другая уязвимость связана с наличием повышенных прав в атакуемой системе. Речь идет не только о возможном доступе к различным сетевым ресурсам, но и о работе в системе с излишними правами, которые не требуются для выполнения задач. Все это может усугубляться сопутствующими проблемами в инфраструктуре: не работает резервное копирование, отсутствует система мониторинга и предупреждения сетевых угроз, неправильно настроено сетевое оборудование и т. п.

## **МЕРЫ ПО ЗАЩИТЕ.**

Использование современного антивирусного ПО для защиты компьютеров в организации обязательно, однако не менее важным защитным ресурсом являются люди. Информационная безопасность должна быть неотъемлемой частью корпоративной культуры. Даже небольшие компании, не располагающие отдельными бюджетами на безопасность, могут многократно усилить ее, используя правильную настройку сетевого оборудования, проводя обучение своих сотрудников основам безопасности при работе за компьютером и устанавливая надежное антивирусное ПО.

### На уровне государства

#### **Разглашение государственной тайны**

Государственная тайна — защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Основы защиты государственной тайны регламентируются законом РФ от 21.07.1993 N 5485–1 .О государственной тайне.

### сведения в военной области:

* о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, предусмотренных Федеральным [законом](consultantplus://offline/ref=4D8435A533D1F56129FFC560B3CE582D055147F1C85AA4CB93182180BE71621F72C163DC392ECBF108FAF3E3D5M765J%20) "Об обороне", об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов;
* о планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;
* о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов, их составных частей, делящихся ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения;
* о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;
* о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов;
* о дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состоянии их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке;

### сведения в области экономики, науки и техники:

* о содержании планов подготовки Российской Федерации и ее отдельных регионов к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов;
* об использовании инфраструктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства;
* о силах и средствах гражданской обороны, о дислокации, предназначении и степени защищенности объектов административного управления, о степени обеспечения безопасности населения, о функционировании транспорта и связи в Российской Федерации в целях обеспечения безопасности государства;
* об объемах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанных вооружения, военной техники и другой оборонной продукции;
* о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства;
* о запасах платины, металлов платиновой группы, природных алмазов в Государственном фонде драгоценных металлов и драгоценных камней Российской Федерации, Центральном банке Российской Федерации, а также об объемах запасов в недрах, добычи, производства и потребления стратегических видов полезных ископаемых Российской Федерации (по [списку,](consultantplus://offline/ref=4D8435A533D1F56129FFC560B3CE582D025046F7CF5FA4CB93182180BE71621F60C13BD0382BD5F000EFA5B2932331BD32C568EF3BD44C0FMA65J%20) определяемому Правительством Российской Федерации);

### сведения в области внешней политики и экономики:

* о внешнеполитической, внешнеэкономической деятельности Российской Федерации, преждевременное распространение которых может нанести ущерб безопасности государства;
* о финансовой политике в отношении иностранных государств (за исключением обобщенных показателей по внешней задолженности), а также о финансовой или денежно-кредитной деятельности, преждевременное распространение которых может нанести ущерб безопасности государства;

### сведения в области разведывательной, контрразведывательной и [оперативно-розыскной деятельности](consultantplus://offline/ref=4D8435A533D1F56129FFC560B3CE582D055648F4C459A4CB93182180BE71621F60C13BD0382BD4F10AEFA5B2932331BD32C568EF3BD44C0FMA65J%20), а также в области противодействия терроризму и в области обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты:

* о силах, средствах, об источниках, о методах, планах и результатах разведывательной, контрразведывательной, оперативно-розыскной деятельности и деятельности по противодействию терроризму, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;
* о силах, средствах, об источниках, о методах, планах и результатах деятельности по обеспечению безопасности лиц, в отношении которых принято решение о применении мер государственной защиты, данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения, а также отдельные сведения об указанных лицах;
* о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность;
* об организации, о силах, средствах и методах обеспечения безопасности объектов государственной охраны, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;
* о системе президентской, правительственной, шифрованной, в том числе кодированной и засекреченной связи, о шифрах, о разработке, об изготовлении шифров и обеспечении ими, о методах и средствах анализа шифровальных средств и средств специальной защиты, об информационно-аналитических системах специального назначения;
* о методах и средствах защиты секретной информации;
* об организации и о фактическом состоянии защиты государственной тайны;
* о защите Государственной границы Российской Федерации, исключительной экономической зоны и континентального шельфа Российской Федерации;
* о расходах федерального бюджета, связанных с обеспечением обороны, безопасности государства и правоохранительной деятельности в Российской Федерации;
* о подготовке кадров, раскрывающие мероприятия, проводимые в целях обеспечения безопасности государства;
* о мерах по обеспечению защищенности критически важных объектов и потенциально опасных объектов инфраструктуры Российской Федерации от террористических актов;
* о результатах финансового мониторинга в отношении организаций и физических лиц, полученных в связи с проверкой их возможной причастности к террористической деятельности;
* о мерах по обеспечению безопасности критической информационной инфраструктуры Российской Федерации и о состоянии ее защищенности от компьютерных атак.

## **МЕРЫ ПО ЗАЩИТЕ.**

Для защиты информации государственной тайны обычно применяются комбинированные способы защиты, которые включают технические средства, программные средства, организационные мероприятия и криптографию.

**К**[**организационным мероприятиям**](https://spravochnick.ru/definitions/organizacionnoe-meropriyatie/) можно отнести [пропускной режим](https://spravochnick.ru/definitions/propusknoy-rezhim/), хранение устройств и носителей в сейфе, [ограничение доступа](https://spravochnick.ru/definitions/ogranichenie-dostupa/) посторонних лиц в компьютерные помещения и другие методы защиты информации государственной тайны.

Технические средства по защите информации государственной тайны включают в себя множество аппаратных способов защиты:

* экраны на аппаратуру;
* фильтры;
* ключи для блокировки клавиатуры;
* установка устройств аутентификации – для чтения форм руки, отпечатков пальцев, радужной оболочки глаз;
* [электронные ключи](https://spravochnick.ru/definitions/elektronnyy-klyuch/) на микросхемах.

**К**[**программным средствам**](https://spravochnick.ru/definitions/programmnye-sredstva/) защиты информации государственной относятся такие средства, которые создаются в результате разработки специального программного обеспечения, что не позволяет посторонним лицам получать информацию из системы. К программным средствам относятся:

* блокировка клавиатуры и экрана;
* парольный доступ-задание;
* применение средств парольной защиты BIOS на персональный компьютер.

[**Криптографическими средствами**](https://spravochnick.ru/definitions/kriptograficheskie-sredstva/)**защиты** информации государственной тайны является применение шифрования при вводе в компьютерную систему.

Противостоять [угрозам информационной безопасности](https://spravochnick.ru/definitions/ugroza-informacionnoy-bezopasnosti/) можно на основе формирования и внедрения эффективных систем защиты информации государственной тайны.

**Особое место занимают правовые меры.**

В статье 8 Закона Российской Федерации «О государственной тайне» говорится о трех степенях секретности сведений, которые находятся в режиме государственной тайны, а также соответствующих грифах секретности – секретно, совершенно секретно, особой важности. Присвоение грифа секретности регламентировано Правилами отнесения сведений, которые составляют государственную тайну, утвержденные Постановлением № 870 Правительства РФ.

Допуск граждан РФ и должностных лиц к государственной тайне реализуется в добровольном порядке. Данный допуск предусматривает:

* принятие обязательств на себя перед государством по нераспространению тех сведений, что составляют государственную тайну и что доверены им;
* согласие на временные, частичные ограничения их прав в соответствии с Федеральным законом РФ «О государственной тайне»;
* письменное согласие граждан и должностных лиц на проведение проверочных мероприятий уполномоченными органами;
* определение размеров, видов и порядка предоставления социальных гарантий, которые предусмотрены ФЗ «О государственной тайне»;
* ознакомление с законодательными нормами РФ, которые предусматривают ответственность за его нарушения в сфере государственной тайны;
* принятие решения руководителем предприятия, органа государственной власти, организации или учреждения о допуске оформляемого гражданина к тем сведениям, которые составляют государственную тайну.

#### **Здоровье населения, демографические показатели**

Рассматривая влияние информационных средств на здоровье человека уместно различать три вида здоровья:

### психическое,

### физическое и

### нравственное.

Причем состояние психики и адекватность душевной деятельности являются теми базовыми факторами, на которых главным образом выстраиваются все другие виды человеческих аномалий. Поэтому психическое здоровье заслуживает того, чтобы говорить о нем в первую очередь.

***Психическое здоровье.*** ХХ век дал не только впечатляющие прорывы в технике, но и столь же впечатляющее нарастание числа разнообразия психических болезней. На хроническую усталость, раздражительность, бессонницу, застойную тревогу, депрессию, разного рода комплексы сегодня не может пожаловаться разве что младенец. Стремительно множится число неврозов, депрессивных состояний, других расстройств психики, как и число неожиданных срывов у людей, вроде бы вполне нормальных в повседневной жизни.

Врачи бьют тревогу: здоровых детей уже практически нет, нормой становится их эмоциональное неблагополучие, дети теряют контакт с действительностью. В проблему превращается школьный невроз, и даже невроз дошкольного возраста. Прием детьми антидепрессантов стал почти нормой для некоторых развитых стран. Нарастает острота подростковых коллизий, все больше подростков кончает жизнь самоубийством; множество детей предпочитает стать беспризорниками, не желая вернуться в «нормально обустроенное бытие» под родительский кров.

Согласно выводам всероссийской диспансеризации, «проблема состояния психического здоровья детей в России за последнее десятилетие стала острой медико-социальной проблемой». Рост психических расстройств за последние годы составил 32 %, подростков

– в 1,7 раза. Критический уровень психического здоровья детей и подростков во многом ограничивает возможности получить полноценное образование, снижает показатели годности юношей к воинской службе. По этой же причине около 70 % учащихся общеобразовательных учреждений испытывают значительные трудности в усвоении базовой школьной программы. По данным Министерства обороны РФ, среди заболеваний, послуживших причиной освобождения юношей от призыва на военную службу в 2000 г., более 20 % пришлось на психические расстройства.

По данным Московского НИИ психиатрии, частота пограничных психических расстройств среди детей всех возрастов, воспитанников и учащихся различных образовательных учреждений колеблется (по разным регионам) от 22,5 до 71 %. Эти цифры позволяют считать проблему психического здоровья подрастающего поколения более чем актуальной. Она уже непосредственно влияет на качество трудовых ресурсов страны и ее безопасность.

Собственно, психическое расстройство может быть даже протестом – молчаливым, загнанным внутрь и, в силу своей невысказанности, оборачивающимся разрушительным действием против самого человека, его здоровья. У того, кто не способен протестовать осознанно, бунтует психика.

Предельным выражением этой тенденции является увеличение количества *суицидов.*Уровень числа самоубийств на 100 тыс. населения России вырос с показателя 26,4 в 1990 г. до 39,7 в 2001 г. и превысил число убийств. Продолжает расти число суицидов среди подростков. В 2003 г. покончили с собой 7800 несовершеннолетних. Эта драматическая тенденция сохраняется и сегодня. Для многих из них такая форма протеста оказывается наиболее доступной и поэтому все более распространенной. **Умение защититься от негативной информации и манипулирования – важнейшее средство профилактики суицидов.**

***Физическое здоровье.***В качестве наиболее репрезентативного исследования здоровья школьников можно рассматривать проведенную в 2002 г. всероссийскую диспансеризацию. Из ее итогов следует, что за последние 10 лет общая заболеваемость детей в возрасте до 14 лет выросла в 1,4 раза. Самые высокие темпы роста наблюдаются у болезней костно-мышечной системы – сказывается компьютеризация и малоподвижность (в 2,6 раза), системы кровообращения (в 2,5 раза), эндокринной и мочеполовой системы.

Тенденцией к росту отличаются также показатели заболеваемости подростков. Самую большую группу составляют дети, находящиеся между здоровьем и болезнью – в так называемом «третьем состоянии». У них есть разнообразные функциональные нарушения, не достигшие уровня болезни, но свидетельствующие о напряжении адаптационных ресурсов, повышенном риске возникновения клинически выраженной патологии. Их нельзя отнести к здоровым, но и диагноза хронического заболевания врачи им не поставили.

По данным Н. К. Смирнова, быстрыми темпами ухудшается здоровье школьниц. За 10 лет число здоровых девушек-выпускниц уменьшилось с 28,3 до 6,3 %, то есть более чем в три раза. Почти 40 % юношей по медицинским показаниям не годятся для службы в Вооруженных силах.

По данным специалистов НИИ гигиены и охраны здоровья детей и подростков, в последние годы наметились следующие негативные тенденции:

значительное снижение числа абсолютно здоровых детей (их остается не более 10– 12 %);

стремительный рост числа функциональных нарушений и хронических заболеваний, которые регистрируются более чем у 50–60 % школьников;

резкое увеличение доли патологии органов пищеварения, опорно-двигательного аппарата, почек и мочевыводящих путей (прямое следствие чрезмерного потребления широко рекламируемых пива, «сникерсов», фанты и т. п.);

увеличение числа школьников, имеющих несколько диагнозов (у 20 % старшеклассников в анамнезе их 5 и более).

***Нравственное здоровье.***Происходящая в последние годы смена нравственных приоритетов на материальные с особой губительностью сказалась на нравственном здоровье российского общества. И больше всего в этом процессе пострадало подрастающее поколение.

Преобладающее информационное воздействие на подростков сегодня таково, что они уже не рассматривают труд как главное средство обретения материального благополучия и внутреннего удовлетворения. Все хотят быть богатыми, но никто не хочет работать. Героем молодежи все чаще становятся нувориш, кинозвезда, бандит, сумевшие разбогатеть в одночасье, сразу. Безнравственная или преступная основа такого обогащения мало кого из школьников волнует. Образцом для них служит другое поведение – наглое, агрессивное, с элементами вседозволенности. Слабому не помогают, а пытаются максимально использовать его беспомощность в своих интересах. По словам Н. К. Смирнова, «пронизывая школу, этот безнравственный прагматизм подвергает наибольшему разрушению именно неокрепшие детские души».

В общении между школьниками вышли из употребления понятия «совесть», «честь», «душевность», «бескорыстность». На слуху теперь иная терминология и иные средства разрешения споров. Многих девушек уже не смущает безнравственность легкого поведения: профессия проститутки для 23 % выпускниц школ видится вполне допустимой при условии высоких заработков. И это не случайно – сегодня они живут среди потоков соответствующей информации, а точнее, в зоне «информационного отравления».

**Приоритеты демографической политики в области охраны здоровья и увеличения продолжительности жизни населения**

В области укрепления здоровья и увеличения продолжительности жизни населения определены следующие приоритеты:

### укрепление состояния здоровья детей и подростков, прежде всего за счет совершенствования профилактических мероприятий по снижению травм и отравлений, курения, алкоголизма и наркомании, развития физической культуры, отдыха и оздоровления;

### сохранение репродуктивного здоровья населения путем совершенствования профилактической и лечебно-диагностической помощи;

### улучшение состояния здоровья населения в трудоспособном возрасте, в первую очередь за счет профилактических мероприятий по снижению травм и отравлений, а также раннему выявлению болезней системы кровообращения, новообразований и инфекционных болезней;

### сохранение здоровья пожилых людей, для которых наиболее важны профилактика сердечно-сосудистых, онкологических, эндокринных и инфекционных заболеваний.

**Инструменты демографической политики, направленные на укрепление здоровья и снижение смертности**

### Финансово-Экономические

### организация прививок и медицинских осмотров

### осуществление различных профилактических мероприятий

### реализацию запретительных мероприятий с целью охраны здоровья

### Хозяйственные

### обеспечение техническими и иными средствами реабилитации

### социальное обслуживание на дому, в полустационарной форме или в стационарной форме

### предоставление лекарственных препаратов и медицинских изделий

### санаторно-курортное лечение

### предоставление жилых помещений

### Информационно-Мотивационные

### просвещение и информирование граждан

### профилактические беседы

### пропаганда навыков здорового образа жизни

### Нормативно-Правовые

### разработка и реализация программ формирования здорового образа жизни и программ реабилитации

### государственный надзор за соблюдением законодательства РФ в сфере охраны здоровья

## **МЕРЫ ПО ЗАЩИТЕ.**

Необходимо возродить систему массового санитарно-гигиенического просвещения и обучения граждан.

Важнейшей задачей является внедрение в практику жизнесохранительного поведения, формирование здорового образа жизни у всех категорий населения. В этой связи необходимо активизировать работу по организации и проведению пропагандистской работы, в том числе через средства массовой информации, направленной на пропаганду здорового образа жизни, что предполагает развитие учреждений физической культуры, отдыха и туризма, досуговых центров (особенно для детей, подростков и молодежи). Следует обеспечить поддержку благотворительных акций и инициатив, ставящих своей целью укрепление здоровья населения. Эти индивидуальные инициативы и благотворительные акции могут стать важным резервом в борьбе с факторами преждевременной и предотвратимой смертности населения. Необходимо разработать механизмы поддержки подобных инициатив.

Особое внимание должно быть уделено снижению потребления алкоголя и принятию мер, направленных на ослабление последствий пьянства и алкоголизма, при этом сочетание мер из области фискальной политики, административных ограничений, информационных воздействий способно привести к желаемому эффекту. Система мер должна включать жесткий контроль качества алкогольной продукции и политику цен, стимулирующую переход к потреблению менее вредных типов алкогольных напитков. Ценовая политика должна, с одной стороны, не допустить переориентацию населения на самодельные или нелегальные алкогольные изделия, но, в тоже время, ограничивать потребление алкоголя.

В этих целях также необходимо введение правил, запрещающих продажу алкоголя лицам, находящимся в состоянии сильного опьянения и несовершеннолетним, запрет на продажу крепких алкогольных напитков в местах массового скопления населения.

Следует усилить контроль за рекламой, имея в виду, что молодежь не должна быть задействована в рекламных роликах спиртных и слабоалкогольных напитков.

В рамках мероприятий по улучшению психического здоровья населения необходимо принятие мер по предотвращению и профилактике самоубийств, которые могут включать создание новых и поддержку существующих телефонов доверия, совершенствование методов работы врачей-психиатров, медицинских психологов, психотерапевтов, социальных работников.

В области охраны и укрепления здоровья граждан будет усилено внимание органов государственной власти Российской Федерации к совершенствованию организации и развитию государственной и негосударственной форм оказания медицинской помощи населению, реализация федеральных программ.

Требует решения проблема обеспечения доступности медицинской помощи больным с тяжелыми заболеваниями, нуждающимся в обследовании и лечении с применением дорогостоящих технологий, в первую очередь в федеральных медицинских учреждениях.

Необходимо обеспечить дальнейшее развитие и укрепление консультационно-диагностических служб областных, краевых и республиканских учреждений здравоохранения, восстановить работу выездных бригад поликлиник с целью обеспечения доступности медицинской помощи жителям сельской местности и отдаленных районов, развивать сеть реабилитационных (восстановительных) отделений центральных районных и районных больниц, а также сети больниц и отделений медико-социальной помощи в сельской местности.

Первоочередной задачей является усиление роли первичной медико-санитарной помощи, структурно-экономические преобразования амбулаторно-поликлинического звена, рациональное использование коечного фонда (уменьшение объемов дорогостоящей стационарной помощи при одновременном увеличении объемов услуг дневных стационаров).

Органами здравоохранения и социальной защиты населения должны реализовываться комплексные меры по дальнейшему развитию психиатрической и наркологической помощи населению, вакцинопрофилактике, борьбе с ВИЧ-инфекцией, туберкулезом, болезнями, передаваемыми половым путем.

Необходимо усилить государственную поддержку мер, направленных на профилактику, раннее выявление заболеваний, разработку и внедрение современных технологий в лечебно-диагностические процессы.

В целях снижения осложнений и смертности от злокачественных новообразований требуются разработка и внедрение скрининговых программ по профилактике и раннему выявлению онкологических заболеваний.

Особое внимание должно быть обращено на профилактику и лечение бесплодия, в связи с чем планируется разработать соответствующие программы, направленные на обеспечение ранней диагностики и лечения нарушений репродуктивного здоровья.

С целью профилактики патологии беременности и родов, сохранения здоровья новорожденных должны быть внедрены паспорта здоровья семьи, предусмотрены возможности повышения качества питания беременных, оздоровления их в санаторно-курортных учреждениях.

Важным направлением является разработка и внедрение прогрессивных организационных и перинатальных технологий, способствующих повышению качества медицинской помощи беременным и новорожденным, развитие перинатальных центров; разработка и внедрение в практику эффективных медицинских технологий диагностики, лечения и реабилитации нарушений репродуктивной функции; разработка и внедрение стандартов по охране репродуктивного здоровья; проведение мероприятий по профилактике нежелательной беременности, абортов и инфекций, передаваемых половым путем.

Особое внимание должно уделяться охране репродуктивного здоровья подростков, созданию и развитию новых подходов к гигиеническому и нравственному их воспитанию.

В связи с широким распространением среди детей и подростков алкоголизма, наркомании, токсикомании, инфекций, передаваемых половым путем, следует предусмотреть создание таких новых структурных подразделений, как отделения (кабинеты) медико-социальной помощи в амбулаторных - поликлинических учреждениях и учебных заведениях.

В целях предотвращения риска нарушения репродуктивного здоровья работающих, должен быть осуществлен комплекс мер, предусматривающих аттестацию рабочих мест для выявления и устранения воздействия неблагоприятных факторов на здоровье работников, проведения сертификационных работ по охране труда. Необходимо предусмотреть в законодательстве ответственность работодателей и других официальных лиц за сокрытие информации о риске для здоровья работающих во вредных и тяжелых условиях.

Кроме того, органами государственной власти должна быть разработана система принципов экономической заинтересованности работодателей в улучшении условий и охране труда, предусматривающая развитие страхования от производственного травматизма.

Обеспечение безбарьерной среды обитания для лиц с ограниченными возможностями требует дальнейшего развития реабилитационной индустрии, направленной на создание возможностей максимального использования потенциала инвалидов.

С целью проведения медико-социальной реабилитации категорий населения, которые в силу жизненных обстоятельств попали в сложные условия существования, необходимо предусмотреть развитие новых форм медико-социального обслуживания граждан из числа освободившихся из мест лишения свободы, а также бездомных, направленных в учреждения социального обслуживания из приемников-распределителей органов внутренних дел. Следует предусмотреть развитие сети Домов ночного пребывания, в которых оказывается социально-психологическая, юридическая помощь гражданам, оказавшимся в трудной жизненной ситуации, не имеющим места жительства и работы.

Активные меры должны быть приняты по развитию и совершенствованию реабилитационной помощи, развитию санаторно-курортных организаций и оздоровительных учреждений системы социальной защиты населения, здравоохранения, образования.

Для улучшения качества и доступности медицинской помощи сельскому населению существенное значение имеет укрепление материально-технической базы лечебно-диагностических комплексов, работающих в сельской местности. Одной из первоочередных задач для органов здравоохранения субъектов Российской Федерации является дальнейшее развитие передвижных форм лечебно-диагностической и консультативной помощи.

#### **Воздействие на сознание людей с помощью пропаганды через информационные ресурсы**

### Контентные методы

### Контекстные методы.

### Контентные методы - это мастерские режиссеры медиа-материалов, работающие за кулисами. Они создают или творчески переосмысливают информацию, выстраивая сюжеты и сценарии, которые могут влиять на общественное мнение. Это искусство наложения своего собственного взгляда на мир через зеркало контента, предлагая аудитории новые перспективы, картины и идеи.

Контентные методы пропаганды включают:

* **Фальсификация**- это подделка или искажение фактов, данных, документов, изображений, видео или других видов информации с целью ввести в заблуждение или обмануть получателей. Примерами фальсификации могут быть подделка цитат или высказываний известных личностей, подмена или редактирование фотографий или видеозаписей событий, создание ложных свидетельств или доказательств и т.д.
* **Дезинформация** - это распространение ложной или недостоверной информации с целью ввести в заблуждение или обмануть получателей. Дезинформация может быть создана или распространена как сознательно (с целью манипуляции), так и несознательно (из-за ошибки или невежества). Примерами дезинформации могут быть ложные новости или слухи о политических событиях, социальных проблемах, здоровье, науке и т.д.
* **Мисинформация**- это распространение правдивой или достоверной информации в неправильном контексте или с неправильной интерпретацией с целью ввести в заблуждение или обмануть получателей. Мисинформация может быть создана или распространена как сознательно (с целью манипуляции), так и несознательно (из-за ошибки или невежества). Примерами мисинформации могут быть вырывание из контекста цитат или высказываний известных личностей, использование устаревших или непроверенных данных или документов, переиначивание смысла или цели информации и т.д.
* **Селективность** — это выборочное представление или упоминание только тех фактов, данных, документов, изображений, видео или других видов информации, которые подтверждают или подкрепляют желаемое сообщение или точку зрения. Селективность может быть использована как для скрытия или игнорирования противоречивой или опровергающей информации (омиссия), так и для акцентирования или усиления желаемой информации (эмфазис). Примерами селективности могут быть использование только положительных отзывов о продукте или услуге.
* **Фрейминг**- это представление или интерпретация информации или медиа-контента в определенном ракурсе или под определенным углом зрения с целью воздействия на восприятие или оценку получателей. Фрейминг может быть использован как для акцентирования или усиления определенных аспектов или характеристик информации (позитивный или негативный фрейминг), так и для создания или изменения ассоциаций или импликаций информации (символический или метафорический фрейминг). Примерами фрейминга могут быть использование эмоционально окрашенных или нейтральных слов для описания одного и того же события, использование метафор или аналогий для объяснения сложных или абстрактных понятий, использование заголовков или подзаголовков для формирования первого впечатления о содержании статьи и т.д.
* **Спин**- это представление или интерпретация информации или медиа-контента в выгодном или невыгодном свете с целью воздействия на отношение или поведение получателей. Спин может быть использован как для уменьшения или увеличения значимости или последствий информации (деминимизация или максимизация), так и для перевода внимания или ответственности, с одной стороны, на другую (отвлечение или перекладывание вины). Примерами спина могут быть использование эвфемизмов или гипербол для описания положительных или отрицательных результатов действий, использование статистических данных или графиков для подтверждения или опровержения утверждений, использование аргументов ad hominem (Апелляция к личности) или straw man (Подмена тезиса) для дискредитации или опровержения оппонентов и т.д.
* **Агитация**— это активное распространение информации или медиа-контента с целью возбуждения эмоций, страстей, интересов или действий получателей. Агитация может быть использована как для мобилизации или стимулирования получателей к поддержке или участию в каком-либо движении, кампании, акции и т.д. (позитивная агитация), так и для демобилизации или демотивации получателей от поддержки или участия в каком-либо движении, кампании, акции и т.д. (негативная агитация). Примерами агитации могут быть использование призывов к действию, лозунгов, плакатов, баннеров, видеороликов и т.д.

### Контекстные методы пропаганды - это сценографы нашего цифрового театра, мастерски манипулирующие кулисами и светом, чтобы создать определенную атмосферу вокруг представленной информации. Они работают с условиями передачи, получения или обработки информации, манипулируя контекстом, чтобы воздействовать на общественное мнение.

Это как директоры сцены, управляющие освещением, звуками и декорациями, чтобы усилить впечатление от представления. Их методы меняют ракурс нашего взгляда на информацию, открывая новые, неожиданные углы. Вот некоторые из контекстных трюков, которые они используют:

* **Цензура**- это ограничение доступа к информации или медиа-контенту по различным критериям, таким как политическая целесообразность, законность, нравственность, безопасность и т.д. Цензура может быть осуществляться как официально (с помощью законодательства, регуляторов, судов и т.д.), так и неофициально (с помощью самоцензуры, давления со стороны общественности, спонсоров, рекламодателей и т.д.). Цензура может быть использована как для запрета или удаления нежелательной или опасной информации или медиа-контента (негативная цензура), так и для разрешения или продвижения желательной или полезной информации или медиа-контента (позитивная цензура). Примерами цензуры могут быть блокировка или фильтрация сайтов, постов, комментариев и т.д., удаление или редактирование контента по требованию правообладателей или властей, запрет или ограничение публикации или распространения контента по определенным темам или категориям и т.д.
* **Модерация** - это контроль качества, релевантности, соответствия правилам или стандартам информации или медиа-контента на различных платформах для общения и выражения мнений в интернете. Модерация может быть осуществляться как автоматически (с помощью алгоритмов, программ, ботов и т.д.), так и вручную (с помощью модераторов, администраторов, редакторов и т.д.). Модерация может быть использована как для предотвращения или устранения нарушений правил или стандартов информации или медиа-контента (негативная модерация), так и для поощрения или поддержания соблюдения правил или стандартов информации или медиа-контента (позитивная модерация). Примерами модерации могут быть проверка или подтверждение источников, данных, документов и т.д., выделение или скрытие контента по определенным критериям (например, популярности, новизне, рейтингу и т.д.), удаление или редактирование контента по жалобам пользователей или властей, вынесение предупреждений или санкций за нарушение правил и т.д.
* **Манипуляция**- это воздействие на психологические процессы восприятия, памяти, мышления, эмоций или поведения пользователей с помощью различных технологий в интернете. Манипуляция может быть осуществляться как явно (с помощью прямых приемов воздействия), так и скрыто (с помощью косвенных приемов воздействия). Манипуляция может быть использована как для формирования или изменения мнений, убеждений, ценностей или предпочтений пользователей (когнитивная манипуляция), так и для стимулирования или подавления эмоций, страстей, интересов или действий пользователей (эмоциональная манипуляция). Примерами манипуляции могут быть использование персонализации или сегментации контента под интересы или предпочтения пользователей, использование алгоритмов ранжирования или рекомендации контента для формирования повестки дня или эффекта пузыря, использование искусственного интеллекта или машинного обучения для создания или изменения контента (например, генерация текста, изображений, видео и т.д.), использование нейромаркетинга или нейропрограммирования для воздействия на подсознание или бессознательное пользователей и т.д.

## **МЕРЫ ПО ЗАЩИТЕ.**

**Способы защиты от пропаганды в интернете**

В этой кибер-арене, где пропаганда искривляет реальность, наш арсенал защиты можно разбить на две стратегические линии: техническую и критическую.

Техническая линия защиты это наш личный щит и меч в борьбе с пропагандой. Это специальные инструменты, программы, приложения и сервисы, которые, как ловкие детективы, проверяют, анализируют, фильтруют и блокируют подозрительную информацию или медиа-контент. Они являются нашими гаджетами-супергероями, которые помогают нам защищаться от наводнения пропагандой в интернете. Вот некоторые из них:

* **Верификация**- это проверка достоверности, правдивости, актуальности или источника информации или медиа-контента с помощью различных методов, таких как сравнение с другими источниками, поиск по ключевым словам или фразам, использование обратного поиска по изображениям или видео и т.д. Верификация может быть осуществляться как вручную (с помощью собственных знаний или навыков), так и автоматически (с помощью специализированных сайтов, программ, приложений или сервисов). Примерами верификации могут быть использование сайтов-фактчекеров (например, Snopes.com, Factcheck.org и т.д.), использование программ-антиплагиаторов (например, Turnitin.com, Copyscape.com и т.д.), использование приложений-детекторов фальшивых новостей (например, Fake News Detector, Fake News Buster и т.д.) и т.д.
* **Аналитика**- это анализ качества, релевантности, соответствия правилам или стандартам информации или медиа-контента с помощью различных методов, таких как оценка достоверности источника, оценка аргументации и логики сообщения, оценка эмоциональной окраски или манипулятивности сообщения и т.д. Аналитика может быть осуществляться как вручную (с помощью собственных знаний или навыков), так и автоматически (с помощью специализированных сайтов, программ, приложений или сервисов). Примерами аналитики могут быть использование сайтов-анализаторов медиа (например, Media Bias/Fact Check, AllSides.com и т.д.), использование программ-анализаторов текста (например, Hemingway App, Grammarly и т.д.), использование приложений-анализаторов эмоций (например, Emotion Recognition, Emotion AI и т.д.) и т.д.
* **Фильтрация**— это выборочное представление или упоминание только тех источников информации или медиа-контента, которые соответствуют определенным критериям качества, релевантности, соответствия правилам или стандартам и т.д. Фильтрация может быть осуществляться как вручную (с помощью собственных предпочтений или настроек), так и автоматически (с помощью алгоритмов, программ, ботов и т.д.). Фильтрация может быть использована как для скрытия или игнорирования нежелательной или опасной информации или медиа-контента (негативная фильтрация), так и для выделения или подкрепления желательной или полезной информации или медиа-контента (позитивная фильтрация). Примерами фильтрации могут быть использование настроек конфиденциальности или безопасности для ограничения доступа к определенным сайтам, постам, комментариям и т.д., использование расширений браузера или приложений для блокировки рекламы, трекеров, всплывающих окон и т.д., использование кураторов контента или агрегаторов новостей для выбора интересующих тем или категорий и т.д.
* **Блокировка**— это полное прекращение доступа к информации или медиа-контенту по различным причинам, таким как политическая целесообразность, законность, нравственность, безопасность и т.д. Блокировка может быть осуществляться как официально (с помощью законодательства, регуляторов, судов и т.д.), так и неофициально (с помощью хакеров, активистов, добровольцев и т.д.). Блокировка может быть использована как для запрета или удаления нежелательной или опасной информации или медиа-контента (негативная блокировка), так и для защиты или сохранения желательной или полезной информации или медиа-контента (позитивная блокировка). Примерами блокировки могут быть использование файрволов, прокси-серверов, VPN-сервисов и т.д. для обхода или предотвращения блокировки сайтов, постов, комментариев и т.д., использование DDoS-атак, вирусов, троянов и т.д. для нарушения работы сайтов, постов, комментариев и т.д., использование шифрования, стеганографии, цифровых подписей и т.д. для защиты информации или медиа-контента от просмотра или изменения и т.д.

Критическая линия защиты - это наши суперсилы, которые преображают нас из простых пользователей интернета в информационных ниндзя. Это развитие наших знаний, навыков и способностей, которые помогают нам навыками рыцаря с мечом критического мышления разбираться, оценивать, интерпретировать и использовать информацию или медиа-контент.

Это наш тренировочный лагерь, где мы обучаемся дисциплинам разведки и контрразведки в мире информации. Это превращает нас в информационных воинов, готовых к каждому замыслу пропаганды. Вот некоторые из наших критических навыков:

* **Медиаграмотность** - это способность понимать природу, функции, формы и эффекты медиа в современном обществе, а также критически анализировать, оценивать и использовать медиа-контент для различных целей. Медиаграмотность включает в себя знание основных концепций и терминов медиа, знание прав и обязанностей медиа-потребителей и медиа-производителей, знание технологий и инструментов для создания и распространения медиа-контента, знание стратегий и приемов для анализа и интерпретации медиа-контента, знание способов и критериев для оценки качества и достоверности медиа-контента, знание методов и целей для использования медиа-контента для обучения, развлечения, информирования или воздействия и т.д.
* **Информационная грамотность** - это способность определять информационные потребности, находить, получать, оценивать, организовывать, хранить и использовать информацию из различных источников для различных целей. Информационная грамотность включает в себя знание основных концепций и терминов информации, знание прав и обязанностей информационных потребителей и информационных производителей, знание технологий и инструментов для поиска и получения информации, знание стратегий и приемов для анализа и интерпретации информации, знание способов и критериев для оценки качества и достоверности информации, знание методов и целей для использования информации для обучения, решения проблем, принятия решений или воздействия и т.д.
* **Критическое мышление** - это способность логически анализировать, оценивать, сравнивать, обобщать, обосновывать или выводить суждения или решения на основе имеющихся фактов, данных или доказательств. Критическое мышление включает в себя знание основных концепций и терминов логики, знание правил и стандартов рассуждения, знание типов аргументов и умение определять их силу или слабость, знание типов логических ошибок и умение избегать или исправлять их, знание методов и целей для развития критического мышления и т.д.
* **Эмоциональная грамотность** - это способность понимать, выражать, управлять и использовать свои и чужие эмоции для различных целей. Эмоциональная грамотность включает в себя знание основных концепций и терминов эмоций, знание типов эмоций и умение определять их причины и последствия, знание способов и критериев для выражения эмоций в соответствии с ситуацией и культурой, знание способов и критериев для управления эмоциями в соответствии с целями и потребностями, знание способов и целей для использования эмоций для обучения, коммуникации, мотивации или воздействия и т.д.
* **Саморегуляция** - это способность контролировать свое поведение, мысли и эмоции в соответствии с целями, правилами или стандартами. Саморегуляция включает в себя знание основных концепций и терминов саморегуляции, знание типов саморегуляции и умение выбирать и применять наиболее подходящие для ситуации, знание способов и критериев для постановки целей и планирования действий, знание способов и критериев для мониторинга и оценки прогресса и результатов, знание способов и критериев для корректировки или изменения целей или действий при необходимости.