

## Содержание:

image not found or type unknown



## Введение

По своему главному значению для развития окружающего мира, информация примеряется к важнейшим ресурсам, наряду с сырьем и энергией. В более развитых странах на сегодняшний день люди постепенно переходят на работу, которая больше связана с обработкой информации, чем идут на производительную деятельность.

Вместе со всем это можно отметить и новую тенденцию, которая имеет заключение во всей общественной зависимости и в зависимости одного человека. Именно поэтому на сегодняшний день появляются все больше понятий на тему «Информационная безопасность», «Информационная политика» и много других вещей, которые помогают защитить нашу информацию.

Мне кажется, что в современном нашем мире происходит процесс, сравнимый с процессом исчезновения или ухода на второй план материальных активов и восхождение информационных.

Сейчас развитие каких-то крупных компаний и организаций больше берет вверх в сторону усложнения информационных систем с целью обеспечения максимальной эффективности в ведении бизнеса и передачи информационных потоков, что является сильнейшим конкурентом на рынке технологий. Если рассматривать информацию как товар, можно предположить, что информационная безопасность в целом может привести к значительной мере экономии средств, что плюс, в то время как ущерб, нанесенный ей (безопасности), приводит к материальным затратам. **Приведу достаточно логичный и уместный пример:** Раскрытие технологии и рецепта изготовления оригинального продукта может привести к появлению аналогичного продукта, но от конкурента, и как следствие нарушится информационная безопасность, то есть владелец технологии, а может быть и автор, потеряют часть рынка и тд.

## Основная часть

Исторический период развития человеческого общества, в котором мы живем, описывают как информационную эру (англ. Information Age), или информационную эпоху. Этот период в течение жизни практически одного-двух поколений сменил собой индустриальную эпоху. Если индустриальная эра базируется в основном на производстве и распределении энергии, то информационная основана на микроэлектронных информационных и коммуникационных технологиях и генной инженерии. Новый этап развития цивилизации отличается тем, что его движущей силой стали ценности, созданные знаниями. Возрастание роли и социального воздействия информации привело к появлению нового вида рисков — угроз информационной безопасности и даже кибер войн — информационных сражений.

Предпосылки информационной эры заложила информационная революция, достижения которой сделали возможным создание сложных технических систем, которые позволили обрабатывать просто огромные по сравнению с предыдущими годами объемы информационных данных. Информационная эра (Англ. Information Age, Digital Age, Computer Age, также известная как Эра компьютеров или информационная эпоха) — концептуальная идея о том, что современный век будет характеризоваться широкими возможностями для отдельных лиц свободно передавать/получать информацию и иметь мгновенный доступ к знаниям, что было бы трудно или невозможно в предыдущие эпохи развития человечества.

## Признаки информационного общества

Последствия информационной революции обусловили коренные изменения во всех сферах жизни человека. Вместе с развитием информационного общества состоялся переход от приоритета производства к экономике услуг, в основе которой лежит не производство товаров, а предоставление услуг. В сфере культуры возникает и развивается «массовая культура», ряд субкультур со своими уникальными характеристиками, киберспорт и тому подобное. Растет популярность социальных сетей и интернет-СМИ. Новейшие средства социального взаимодействия, возрастание роли средств массовой информации в организации общества создали новые формы правления обществом — нетократии и медиакратии. Основной ценностью для общества в целом и отдельного человека в частности постепенно становятся информационные ресурсы. Это, в свою очередь, вызывает потребность в уточнении понятия информация.

Информацию как объективное явление можно рассматривать и по таким признакам:

- это самостоятельная производственная отрасль, то есть вид экономической деятельности;
- это неотъемлемый фактор любого производства, который является фундаментальным ресурсом каждой экономической системы;
- это информационный продукт, который лежит в основе создания информационного продукта или информационной услуги и выступает как материальный товар, определяется не стоимостью, а монопольной ценой через равновесие спроса и платежеспособности покупателя;
- это элемент рыночного механизма, который наряду с ценой и полезностью влияет на определение оптимального состояния экономики и ее равновесия;
- это один из важнейших факторов в конкурентной борьбе.
- Информация влияет на эффективность производства без физического увеличения традиционных ресурсов; действует на субъективный фактор производства — человека, его характер, особенности; ускоряет процесс производства благодаря уменьшению периодов производства и обращения.

Исходя из такого понимания информации, определим основные признаки информационного общества:

- Преобразование информации в важнейший экономический ресурс, имеет глобальный характер и обеспечивает повышение эффективности, рост конкурентоспособности и инновационное развитие субъектов хозяйствования. Ведущим видом собственности становится собственность человека на информацию как духовный продукт; знания и информация приобретают свойства товара. Преобразование информационной сферы в фундамент, основу всех видов экономической деятельности в XXI в. Информационное общество видом открытого общества, характеризующееся доступностью информации для граждан; возрастание роли информационного менеджмента в управлении обществом и различными сферами жизни.
- Информация развивается по своим законам, не связанными с реальными фактами (ложная информация способна вносить серьезные изменения в жизни людей и общественно-политические процессы).

Таким образом, информационное общество — это общество, в котором большинство работающих занято производством, хранением, обработкой и распространением информационных данных.

Кроме положительных моментов информационного общества можно выделить и опасные тенденции:

- все большее влияние на общество средств массовой информации;
- информационные технологии могут разрушить частную жизнь людей и организаций;
- существует проблема отбора достоверных информационных данных;
- многим людям будет трудно адаптироваться к среде информационного общества;
- существует опасность разрыва между людьми, занимающимися разработкой информационных технологий, и потребителями.

## **Существующие угрозы информационной безопасности**

Угрозой информационной безопасности называют любые обстоятельства или события (атаки), которые могут быть причиной нарушения целостности, конфиденциальности или доступности информации и создающие опасность жизненно важным интересам личности, общества и государства в информационной сфере.

Попытка реализации угрозы по компьютерной системе или сети называют атакой (хакерской атакой, кибератакой). Хакерская атака — действия киберзлоумышленников или вредоносной программы, направленные на захват, удаления или редактирования информационных данных удаленной системы, получение контроля над ресурсами системы или на вывод ее из строя.

Угроза информационной безопасности, как и любая угроза состоит из субъекта (нарушителя, пользователя, отдельного гражданина или предприятия), объекта (сайт, сервер, база данных или документ) и вектора атаки (похищение пароля, социальная инженерия и прочее ) и может быть внутренней или внешней. Бывают и случаи, когда к нарушениям приводит ошибка или халатное отношение работника к информации, которой он оперирует. Примером такого нарушения могут быть случаи, когда работники оставляют важные документы в общественном транспорте.

# Защита информации

Защита информации — это совокупность мероприятий, направленных на предотвращение нарушения конфиденциальности, целостности, доступности информации. Например, защита от несанкционированного доступа, использования, публикации, разрушения, внесение изменений, ознакомления, проверки, записи и чтения.

- То есть для того, чтобы правильно построить систему защиты информации, необходимо ответить на несколько вопросов: какую информацию необходимо защищать;
- как злоумышленник может получить к ней доступ;
- каким образом можно воспрепятствовать злоумышленнику?

Каждый метод защиты информации обеспечивает отдельный аспект безопасности, но почти всегда они используются комплексно.

- Технический метод защиты информации — обеспечивает ограничение доступа к информации аппаратно-техническими средствами (антивирусы, фаерволы, маршрутизаторы, токены, смарт-карты и т.д.).
- Инженерный метод защиты информации предупреждает удаления, доступ или изменения информации в результате умышленных действий или естественного влияния инженерно-техническими средствами.
- Организационный метод защиты информации предупреждает доступ на объект информационной деятельности посторонних лиц с помощью организационных мер (правила разграничения доступа).
- Криптографический метод защиты информации предупреждает доступ с помощью математических преобразований сообщение (шифрование отсылаемых сообщений, хеширования паролей).

## Обеспечение информационной безопасности

Для обеспечения защиты граждан каждое государство строит соответствующую информационную политику по информационной безопасности. Информационная политика государства направлена на защищенность жизненно важных интересов человека, общества и государства от причинения вреда через: неполноту, несвоевременности и недостоверность используемой информации; негативное

информационное влияние; негативные последствия применения информационных технологий; несанкционированное распространение, использование и нарушение целостности, конфиденциальности и доступности информации. В Российской Федерации политика обеспечения информационной безопасности регламентируется целым рядом законодательных актов и строится на следующих принципах: ответственность за сохранность информации, ее засекречивание и рассекречивание; обеспечение доступа к информационному ресурсу с учетом определенных Законом прав собственности на этот ресурс; регламентация прав, обязанностей и ответственности всех субъектов информационного пространства; ответственность за сохранность и использование персональных данных и конфиденциальной информации; защита от ложной, искаженной, недостоверной информации; контроль за созданием и использованием средств защиты информации; защита внутреннего рынка от проникновения некачественных средств информатизации и информационных продуктов.

## **Заключение**

Подводя итоги, можно сказать, что в современном мире стремительно развивающихся интернет-технологий, обязательно должны развиваться центры по защите, охране и обеспечению безопасности нашей информации и данных в сети Интернет. Ведь сейчас любой человек, который зарегистрирован на всех необходимых нашей жизни серверах (магазинах, соц.сетях и тд) подвержен большой опасности. Ведь одного антивируса уже недостаточно.

К тому же сейчас очень хорошо распространен фишинг и прочие уловки злоумышленников.

Использование возможных мер по защите информации можно свести к решению трех основных задач:

1. защита информационных потоков между различными офисами компании (шифрование)
2. защищенный доступ удаленных пользователей сети к информационным ресурсам компании, как правило,

осуществляемый через интернет;

1. защита информационных потоков между отдельными приложениями внутри корпоративных сетей (этот аспект также очень важен, поскольку большинство атак осуществляется из внутренних сетей).

## **Список использованной литературы**

- Автоматизированные информационные технологии в экономике Ред.: Г.А.Титоренко Москва: Юнити, 2006.
- Копыл В.И. Поиск в Интернете./ В. И. Копыл.— М.: АСТ,

Мн.: Харвест, 2006.— 64 с.

- <https://knowledge.allbest.ru/programming/2c0a65625a2ac78a5c5>

[За88521216d27\\_0.html](#)

- 5. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. М.: Книжный мир 2009 - 352 с.
- <https://www.polnaja-jenciklopedija.ru/nauka-i-tehnika/informatsionnaya-bezopasnost.html>