Основные правила информационной безопасности и финансовой безопасности

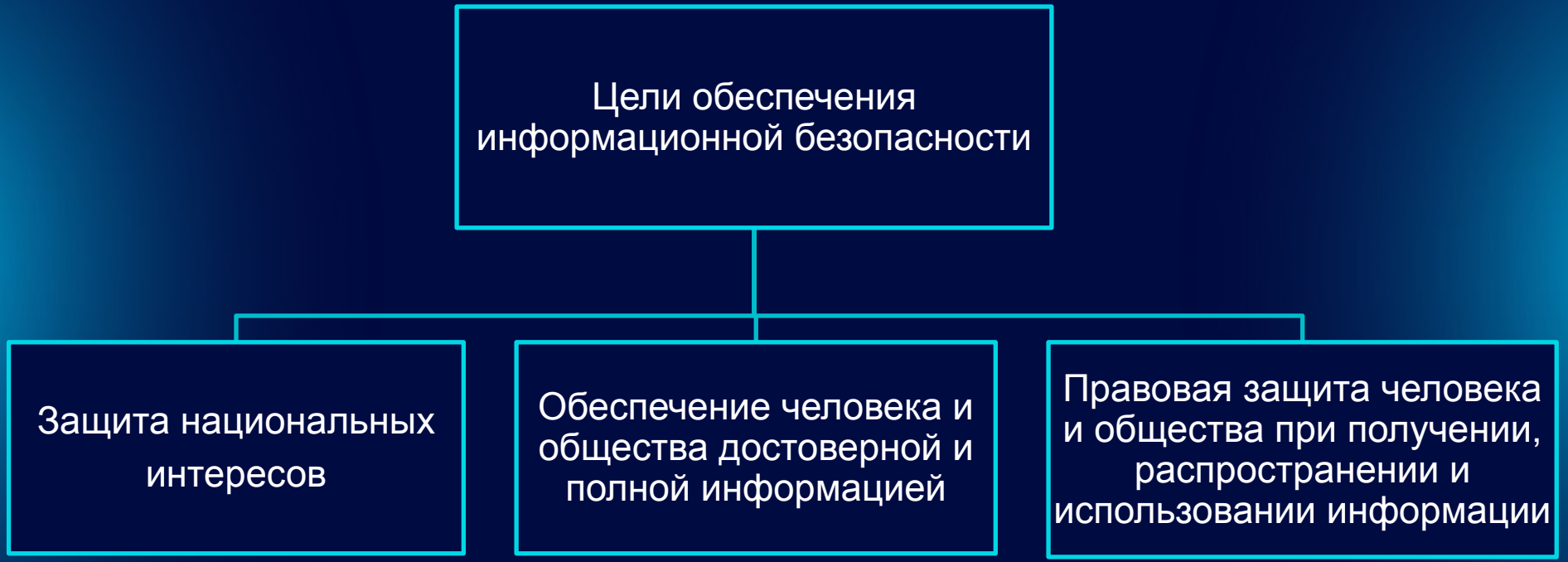
Информационная среда

Это совокупность условий, средств и методов на базе компьютерных систем, предназначенных для создания и использования информационных ресурсов.

Информационная безопасность

Это совокупность методов, инструментов и процессов, которые используются для защиты информации от несанкционированного доступа, утечки, изменения и уничтожения.

Информационная безопасность



Информационная безопасность

- **Информационные**
- **угрозы**
  - Внешние
  - факторы
  - Внутренние
  - факторы

Информационные угрозы

К источникам основных внешних угроз относятся:

- политика стран, противодействующая доступу к мировым достижениям в области информационных технологий;
- «информационная война», нарушающая функционирование информационной среды в стране;
- преступная деятельность, направленная против национальных интересов

Информационные угрозы

К источникам основных внутренних угроз относятся:

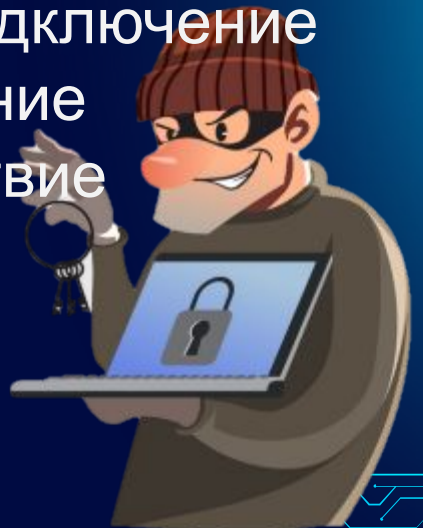
- некоторое отставание от ведущих стран мира по уровню информатизации;
- технологическое отставание электронной промышленности в области производства информационной и телекоммуникационной техники;
- снижение уровня образованности граждан, препятствующее работе в информационной среде

Информационная безопасность

- **Информационные**
- **угрозы**
  - Преднамеренные
  - Случайные

Преднамеренные угрозы

- хищение информации, уничтожение информации;
- распространение компьютерных вирусов;
- физическое воздействие на аппаратуру: внесение изменений в аппаратуру, подключение к каналам связи, порча или уничтожение носителей, преднамеренное воздействие магнитным полем.

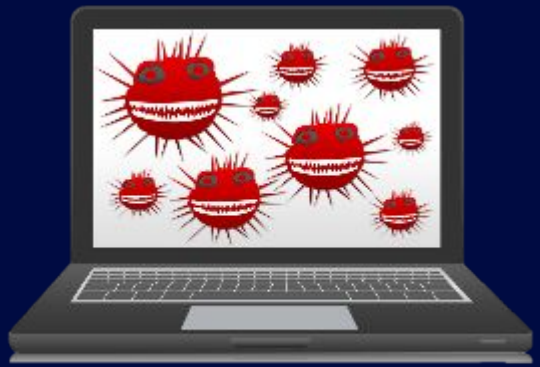


Случайные угрозы

- ошибки пользователя компьютера;
- ошибки профессиональных разработчиков информационных систем;
- отказы и сбои аппаратуры, в том числе помехи и искажения сигналов на линиях связи;
- форс-мажорные обстоятельства (авария, пожар, наводнение и другие так называемые воздействия непреодолимой силы).

Информационные угрозы

Все чаще причиной информационных «диверсий» называют Интернет. Это связано с расширением спектра услуг и электронных сделок, осуществляемых через Интернет. Все чаще вместе с электронной почтой, бесплатными программами, компьютерными играми приходят и компьютерные вирусы.



Основные правила информационной безопасности

- Установите антивирусные программы и периодически обновляйте их.
- Используйте сложные логины и пароли.
- Не публикуйте в соцсетях лишнюю личную информацию. Скройте в настройках приватности номер телефона и адрес электронной почты.

Основные правила информационной безопасности

- Лучше не использовать публичный вайфай (в транспорте, кафе, парках, торговых центрах), который могут взломать и во время сессии передать ваши данные. Пользуйтесь мобильным интернетом на вашем устройстве.
- Если вы использовали чужое устройство, после окончания сессии не достаточно просто закрыть страницу браузера или приложения, необходимо выйти из всех аккаунтов, в которые вы заходили.

Основные правила информационной безопасности

- Безопасность соединения. Обратите внимание на адрес страницы, если он начинается с «http://», а не с «https://», у страницы нет сертификата безопасности. Не оставляйте на этом сайте конфиденциальную информацию. Если адрес сайта начинается с «https://» и слева от него вы видите значок в виде замка, всё в порядке, ваши данные под защитой.

Основные правила информационной безопасности

- Если ваш собеседник представился сотрудником полиции, службы безопасности банка и просит назвать ваши паспортные данные, ПИН-коды, пароли и другие конфиденциальные сведения — не делайте этого. Лучше обратитесь в ту организацию, сотрудником которой представился ваш собеседник, и уточните информацию.

Основные правила информационной безопасности

- Не переходите по подозрительным ссылкам. Даже если видите какое-то очень заманчивое на первый взгляд предложение.
- Не открывайте подозрительные письма. Если вы получили письмо на электронную почту, сначала ознакомьтесь с заголовком и обратите внимание на адресанта — от кого письмо было отправлено.

Основные правила информационной безопасности

- Устанавливайте приложения только из безопасных источников.
- Блокируйте подозрительных собеседников в соцсетях и мессенджерах. Многие мошенники постараются вызвать у вас жалость и обмануть, будьте внимательны.
- Прежде чем отправить что-то личное собеседнику, подумайте, не используют ли ваши данные против вас.

Помните!

Сегодня информация — один из решающих факторов, влияющих на развитие отдельной личности и общества в целом.
Сегодня важно соблюдать правила безопасности не только в реальной, но и в виртуальной жизни.

Финансовая безопасность

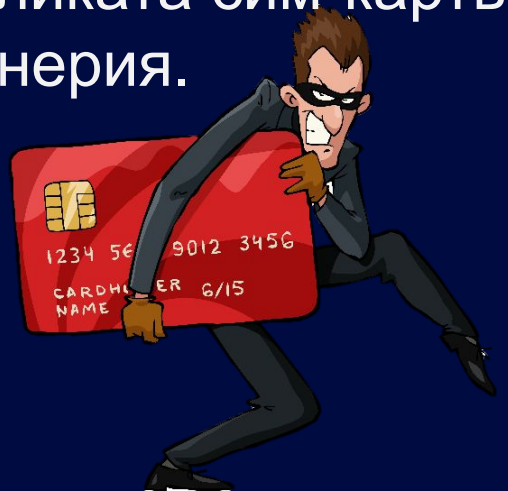
Наша финансовая безопасность напрямую зависит от принимаемых нами ежедневно решений. Непродуманный выбор поставщика финансовых услуг, невнимательное чтение условия договоров, отсутствие финансовой дисциплины и - как следствие - неисполнение своих обязательств и неприятная финансовая ситуация.

Финансовая безопасность личности

Это социально-экономическая возможность человека, иметь финансовую независимость для удовлетворения своих материальных и духовных ценностей, как индивидуально, так и внутри общества, а также сохранение этой независимости в перспективе и её дальнейшее преумножение.

Виды финансового мошенничества

- Кража данных карты при расчете.
- Двойная транзакция.
- Кража денег с карт, оснащенных технологиями бесконтактной оплаты.
- Изготовление дубликата сим-карты.
- Социальная инженерия.



Как избежать кражи данных при расчете

- Не передавать карту посторонним, рассчитываясь за покупку или предоставление услуг.
- Следить за поведением сотрудника, совершающего операцию (подозрительно, если, например, карту фотографируют на мобильный телефон под видом набора номера или СМС).
- Если есть такая возможность, завести для расчетов через Интернет отдельную карту.

Как избежать двойных транзакций

- Подключить опцию СМС-оповещений по операциям своей карты. Если первая транзакция будет совершена успешно, владелец карты тут же получит соответствующее СМС-сообщение.
- Если вам поступило два сообщения о списании одной и той же суммы, стоит сразу же позвонить в банк и проверить, действительно ли произошло двойное снятие средств со счета.

Как избежать кражи денег с карт с технологиями бесконтактной оплаты

- Использовать специальные экранированные бумажники.
- Убедиться, что в качестве подтверждения списания суммы более 1000 рублей стоит запрос PIN-кода, а не подпись чека.
- В случае если вы не планируете оплачивать бесконтактным способом покупки на сумму более 1000 рублей, рекомендуется установить индивидуальный расходный лимит по карте и ограничить размер возможных транзакций.

Что делать при изготовлении дубликата сим-карты?

- В случае получения внезапного оповещения об изменении состояния счета после звонков с неизвестных номеров или на неизвестные номера немедленно блокировать все свои пластиковые карты, привязанные к этому телефонному номеру, позвонив на горячие линии банков, номера которых указаны на самих картах.

Что делать при изготовлении дубликата сим-карты?

- Обратиться к мобильному оператору для разблокировки своей сим-карты и одновременной блокировки дубликата, полученного мошенниками.
- Подать заявление в правоохранительные органы.

Как противодействовать мошеннической социальной инженерии

- Не сообщать данные карты, персональные данные и коды, присланные в СМС, посторонним лицам.
- Ни в коем случае не давать никому доступ к вашей карте через онлайн-банкинг.
- В любых подозрительных ситуациях звонить в кредитную организацию, выдавшую карту.

Помните!

Если Вы стали жертвой финансовых мошенников, немедленно сообщите в полицию.

Спасибо за внимание!