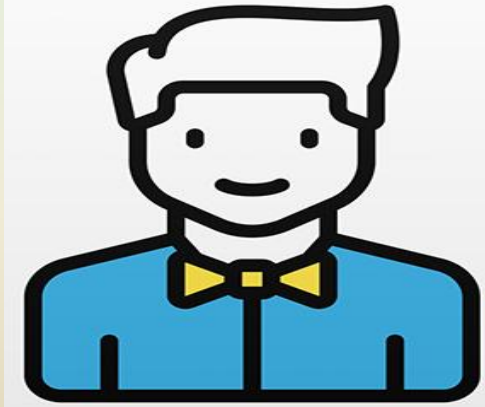
Личная информация, средства ее защиты. Организация личного информационного пространства.

Задачи урока:

1) Ввести понятие личные (персональные) данные.
2) Рассказать способы организации и защиты данных.
3) Выявить правила информационной безопасности.
4) Рассказать про виды угроз и проблемах в Интернете.
5) Привить понимание и осознание, что в Интернете нужно уметь защищаться.

Личная информация. Персональные данные

Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому лицу (п. 1 ст. 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных **данных**"; далее – закон о персональных **данных**).



Персональные данные

- ФИО
- Дата и место рождения
- Адрес
- Семейное, социальное и имущественное положение
- Образование и профессия
- Данные о поведении пользователя на сайте
- Cookie
- Сведения о геопозиции и IP-адрес

https://youtu.be/XZcWkunktAM?t=7

Информационная безопасность личности

Безопасность личности — состояние защищенности ее жизненно важных интересов (совокупность потребностей, удовлетворение которых обеспечивает существование и возможность прогрессивного развития личности) от внутренних и внешних угроз.

Принципы информационной безопасности

1. ***Целостность информационных данных.*** Означает способность информации сохранять изначальный вид и структуру как в процессе хранения, так и после неоднократной передачи. Вносить изменения, удалять или дополнять информацию вправе только владелец или пользователь с легальным доступом к данным.

2. ***Конфиденциальность.*** Характеристика, которая указывает на необходимость ограничить доступ к информационным ресурсам для определенного круга лиц. В процессе действий и операций информация становится доступной только пользователям, которые успешно прошли идентификацию.

3. ***Доступность.*** Означает, что информация, которая находится в свободном доступе, должна предоставляться полноправным пользователям ресурсов своевременно и беспрепятственно.

4. ***Достоверность.*** Указывает на принадлежность информации доверенному лицу или владельцу, который одновременно выступает в роли источника информации.

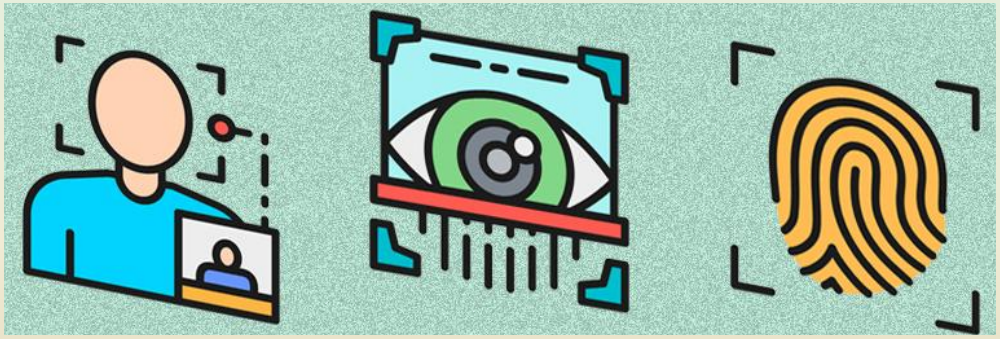
Охрана персональных данных

Международные документы обязывают страны принимать надлежащие меры для охраны персональных данных, накопленных в автоматизированных базах данных, от случайного или несанкционированного разрушения или случайной утраты, от несанкционированного доступа, изменения или распространения.

Компании и государства постоянно обмениваются личными данными, и практически невозможно отследить, кто и какой информацией о людях облада

Внедряются системы для сбора и использования биометрических данных

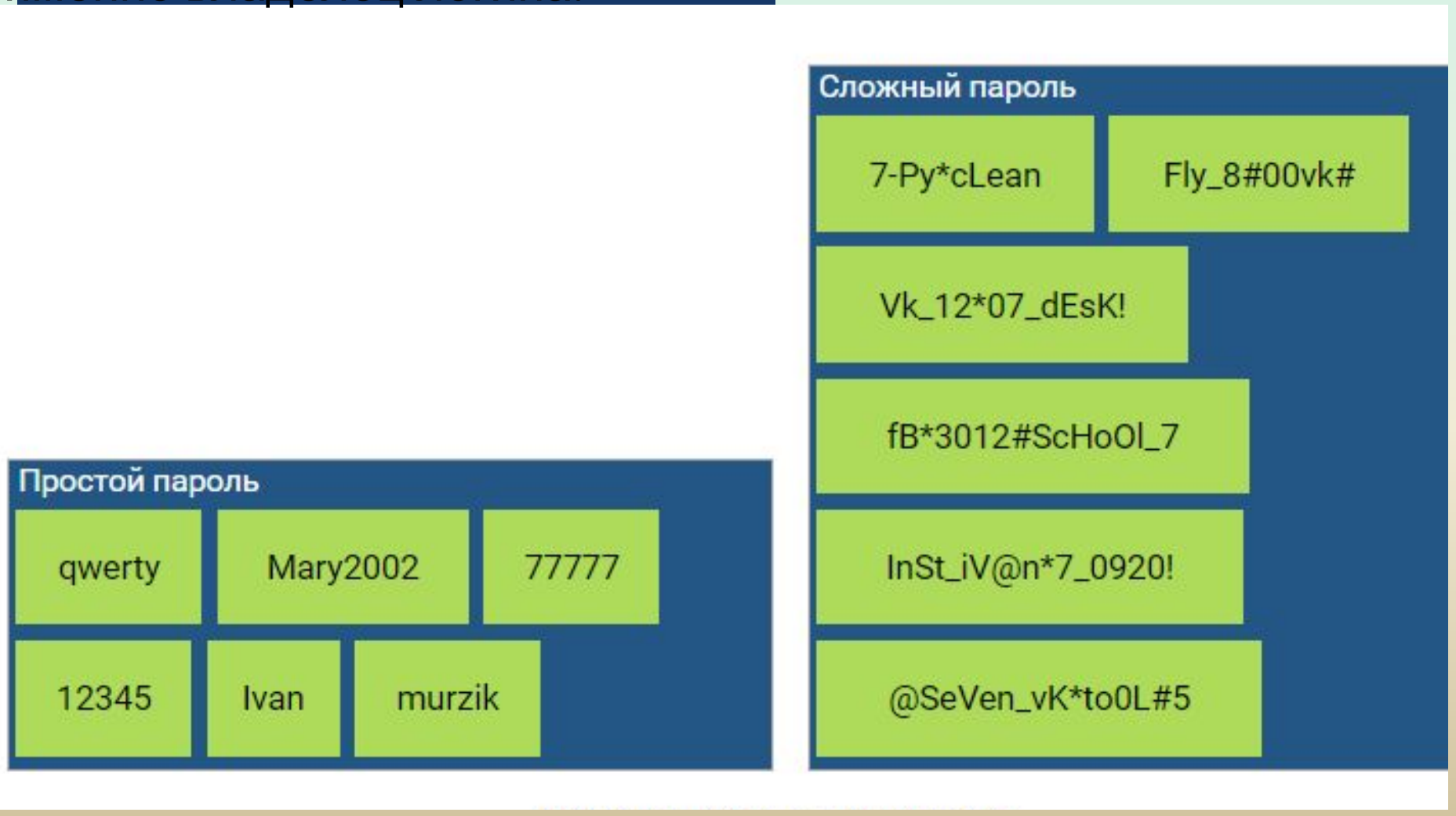
- ДНК
- лицевой геометрии
- голоса
- отпечатков пальцев
- узора сетчатки и радужной оболочки глаза



Камеры видеонаблюдения с системой автоматического распознавания лиц для поиска и маркировки отдельных людей устанавливаются во всем мире. Многие государства осуществляют сбор, хранение и анализ данных о пользователях через электронную почту, телефонные и видеозвонки, текстовые сообщения и посещаемые веб-сайты.

Выбор стойкого пароля

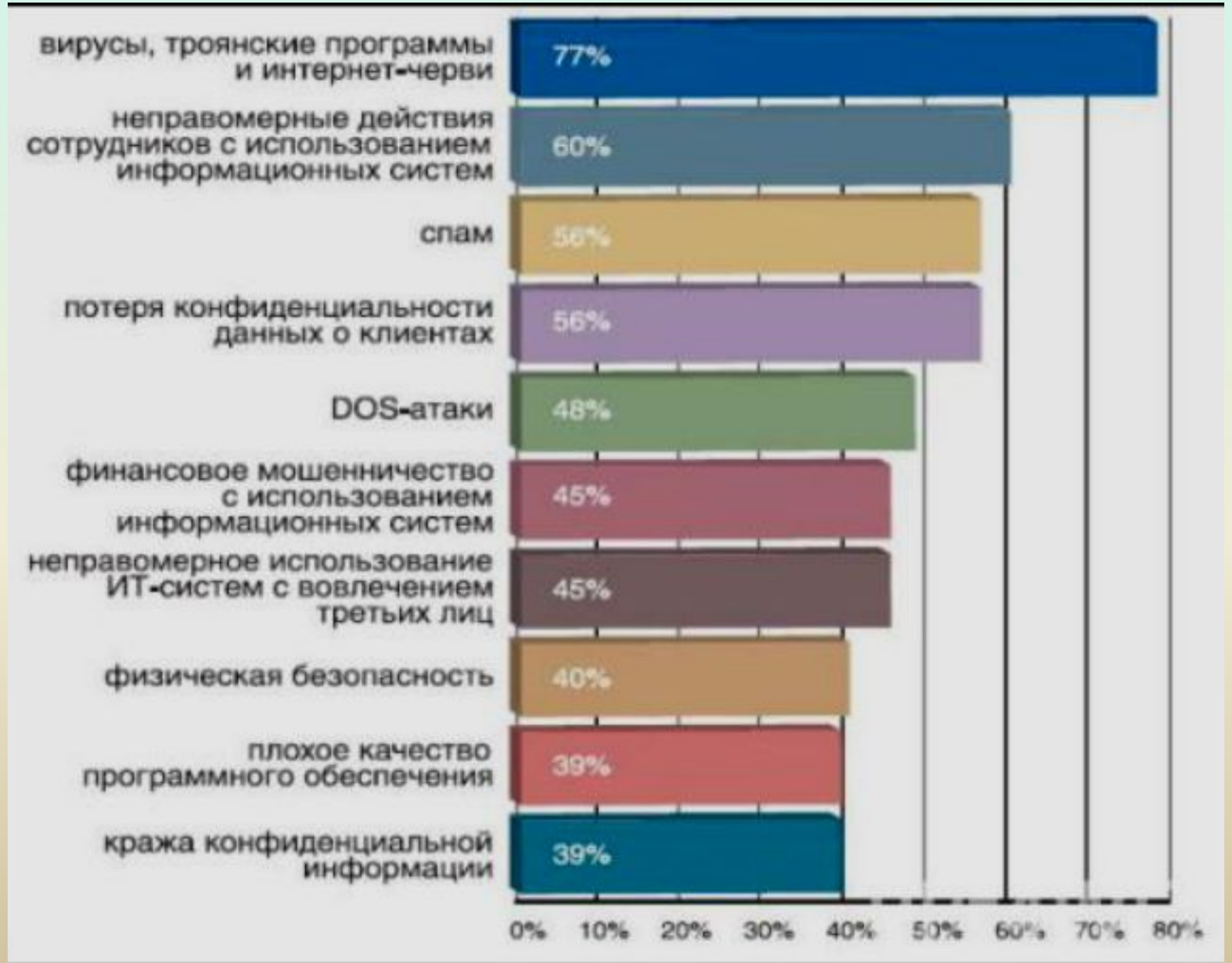
Пароль — это сочетание различных символов, подтверждающих, что логином намеревается воспользоваться именно владелец логина.



Вред и угрозы для персональных данных

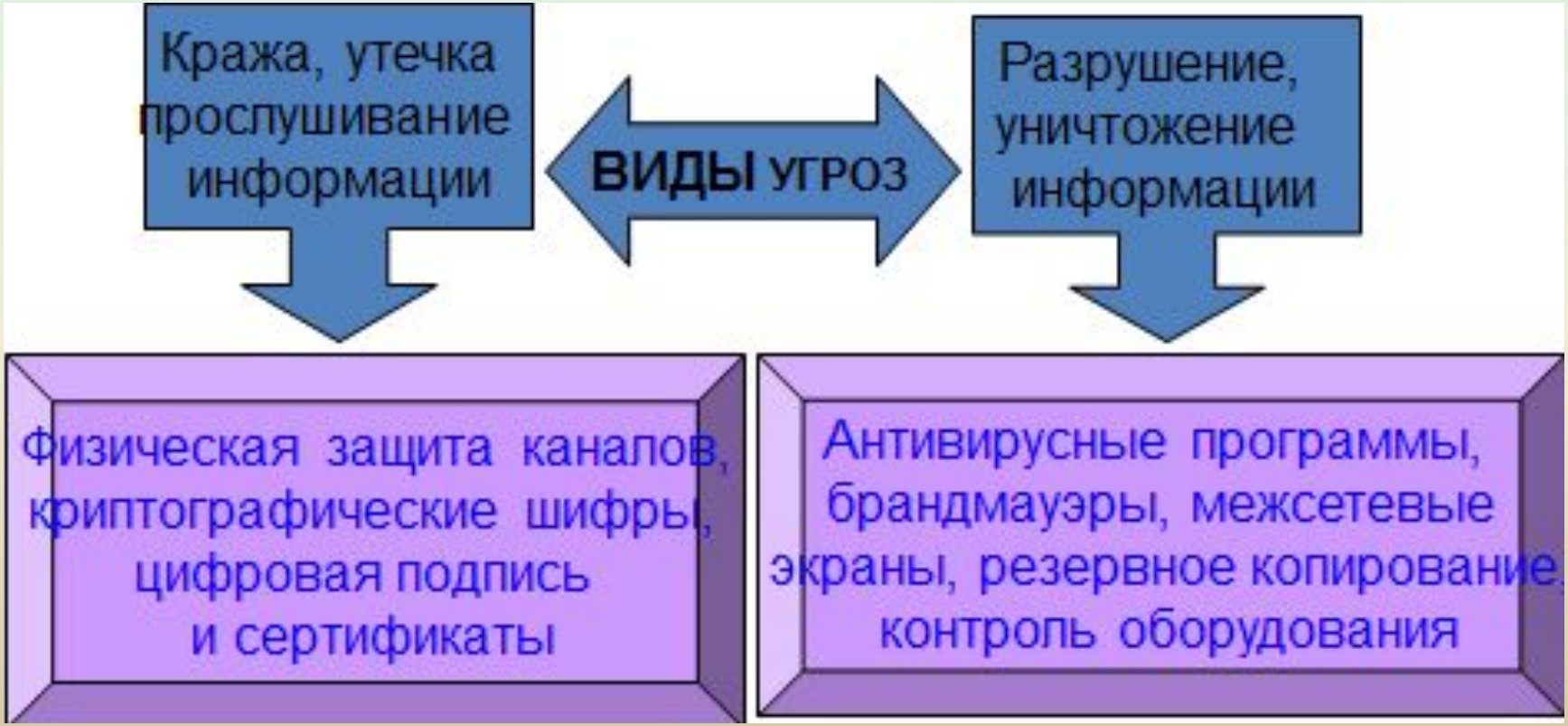
1. Раскрытие паролей
2. Перехват данных
3. Кража оборудования
4. Угрозы конфиденциальности
5. Маскарад – выполнение действий под видом лица, обладающим полномочиями для доступа к данным

10 главных угроз безопасности



Виды угроз

Угроза – это возможность нарушения или нежелательного изменения одного из аспектов информационной безопасности.



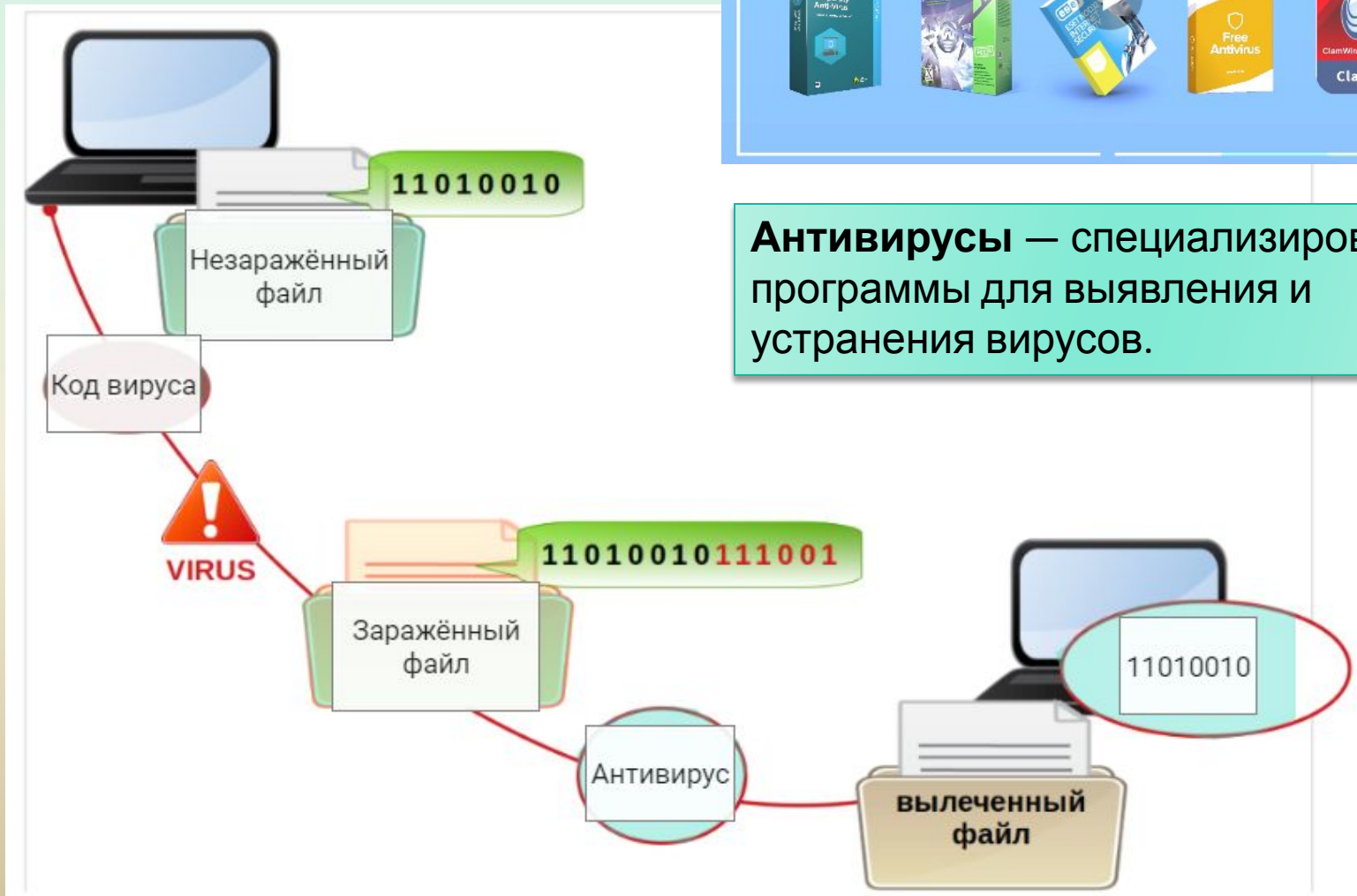
Угрозы безопасности

- ❑ роза утечки (несанкционированного доступа)
- ❑ роза отказа аппаратуры
- ❑ роза некорректной работы программных средств
- ❑угроза невыполненной домашней работы
- ❑угроза со стороны одноклассников
- ❑угроза двойки

Угрозы, исходящие от компьютерных вирусов:

Работа антивируса

Антивирусы — специализированные программы для выявления и устранения вирусов.



Пароли, вирусы, антивирусы

В представленном облаке тэгов выберите стойкие варианты паролей и разместите их в первый столбец, вредоносное программное
обеспечение — во второй столбец, названия антивирусных программ — в третий столбец.

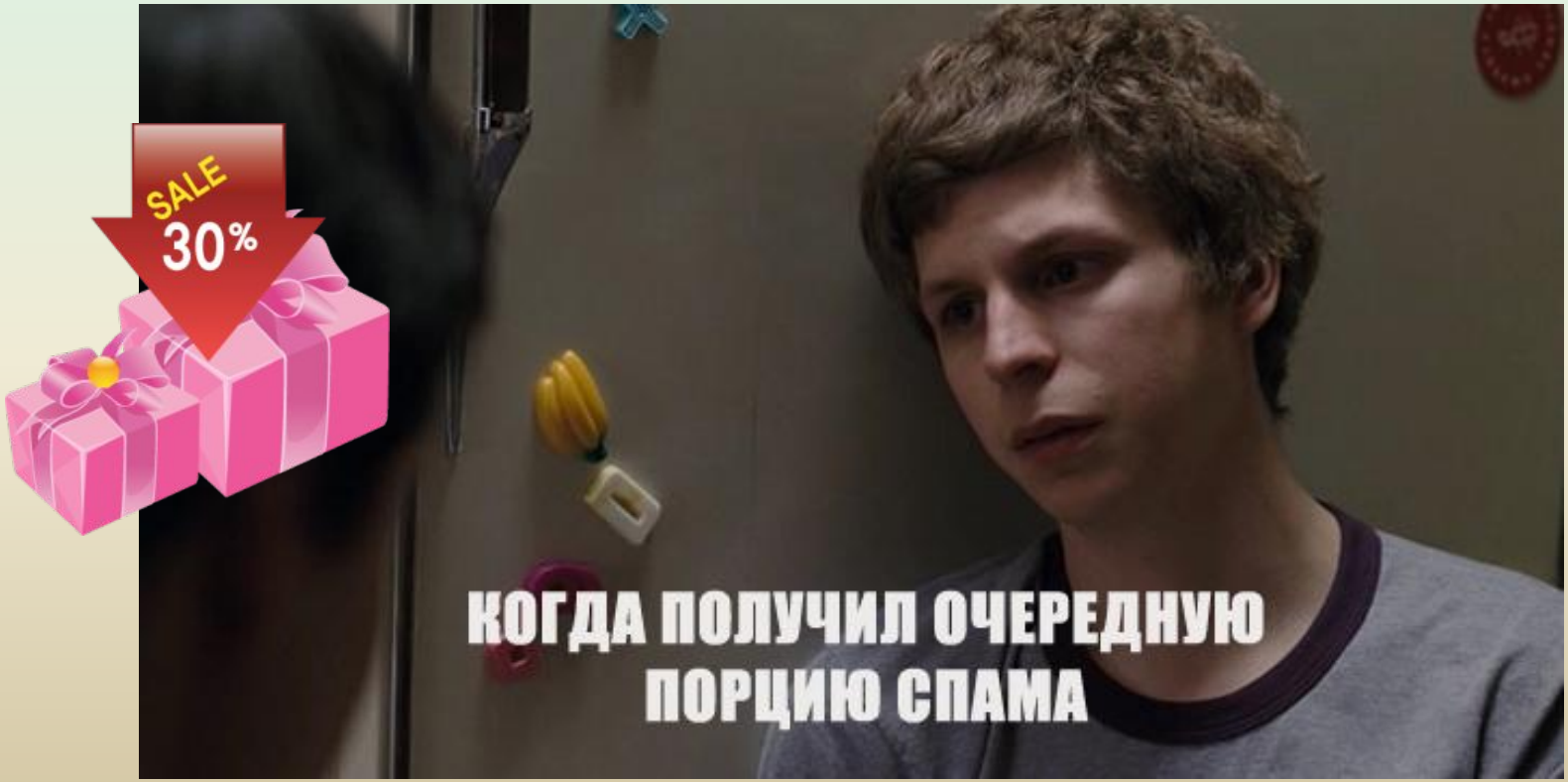
	Вредоносное программное обеспечение	Антивирусные программы
sVet_4$yOu# Nod#Mary-12! Pro*sL_2020	Вирусы Черви Троянцы	Dr. Web NOD32 Avast

История появления слова «спам»

Слово «спам» появилось в 1937 году в результате конкурса на лучшее название для мясных консервов (SPAM — Spiced hAM, ветчина со специями). В военное время огромные залежи консервов поступали по ленд-лизу союзникам: в послевоенной Англии спам стал основным продуктом питания.

Окончательно слово «спам» стало синонимом чего-то навязчивого, надоедливого после показа английской комик-группой в 1972 г. юмористической сценки, сюжет которой был таков: муж с женой приходят в кафе, где все блюда – это спам; окружающие начинают распевать спаму гимн, и пара, доведённая до белого каления, вынуждена взять навязчивый продукт. Сценка была весьма популярной и неудивительно, что с распространением нежелательных рассылок слово опять вспомнилось и

Спам — массовая рассылка корреспонденции рекламного характера лицам, не выражавшим желания её получить. Распространителей спама называют спамерами. В общепринятом значении термин «спам» в русском языке впервые стал употребляться применительно к рассылке электронных писем.



Меры защиты от вредоносных программ

Является мерой защиты от вредоносных

- установить систему антивирусной защиты
- своевременно обновлять систему антивирусной защиты
- проверять флэшку после того, как давал её другу
- не открывать вложений, полученных от неизвестных адресатов с неизвестными целями
- регулярно проводить полную проверку системы

Не является мерой защиты от вредоносных

- не обновлять систему антивирусной защиты
- не проверять флэшку после того, как давал её другу
- не проверять карту памяти друга перед использованием на своём компьютере
- открывать вложение, полученное от неизвестного адресата, но с пометкой «Важно!»
- после установки антивируса можно никогда не проводить полную проверку системы

Организация личного информационного пространства

Информационное пространство пользователя — это информационные ресурсы, доступные пользователю при работе на компьютере.

Результатом воздействия информационных угроз являются:

Информационные угрозы - совокупность факторов, которые представляют опасность для функционирования информационной среды, называют информационными угрозами.

- Несанкционированное ознакомление с информацией
- Исчезновение информации
- Модификация информации

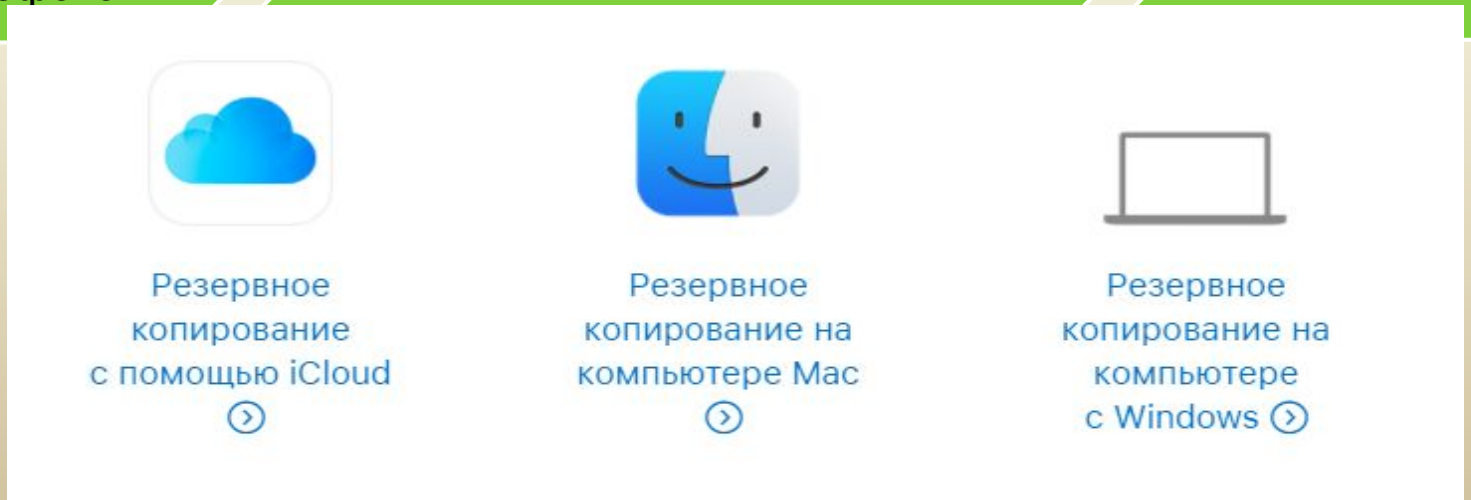
Резервное копирование

Резервное копирование — создание копии данных на носителе (жёстком диске, флешке, телефоне и т. д.), из которых потом можно быстро восстановить состояние системы (в случае повреждения или разрушения данных) и данных на момент, когда эта копия была сделана.

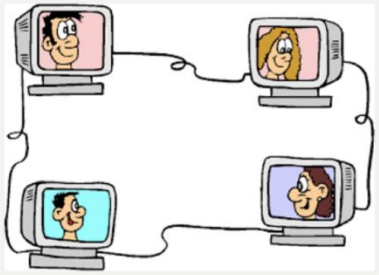
Откройте настройки телефона.

Выберите Система Резервное копирование.

Нажмите Начать копирование



СЕТЕВОЙ ЭТИКЕТ



- Правило 1: Помните, что Вы говорите с человеком.
- Правило 2: Придерживайтесь тех же стандартов поведения, что и в реальной жизни
- Правило 3: Помните, где Вы находитесь в киберпространстве
- Правило 4: Уважайте время и возможности других
- Правило 5: Сохраняйте лицо

Правила информационной безопасности для школьников:

· Придумывая себе имя для Интернета (ник, имя пользователя, логин) вы можете отразить в нем свои стремления, характер, интересы. При этом личную информацию, такую как ваша фамилия или дата рождения, включать в ник не рекомендуется.

· Никому, кроме родителей, не сообщайте свой пароль. При завершении работы с общедоступным компьютером корректно выходите из учетных записей, которые вы использовали.

Правила информационной безопасности для школьников:

· Никому не сообщайте личную информацию (фамилию, домашний адрес, номер телефона, название школы и т. д.), не публикуйте в сети фотографии или видеоролики без одобрения ваших родителей.

· Поскольку каждый пользователь интернета может опубликовать любую информацию, не все, что вы видите в Сети, верно. Старайтесь мыслить критически, чтобы оценить достоверность материалов. Обсуждайте с учителями, школьным библиотекарем, родителями вопрос о безопасных и достоверных интернет-источниках информации, которые можно использовать для решения учебных задач.

Правила информационной безопасности для школьников:

· Опасайтесь интернет-мошенничества: получив сообщение о выигрыше или возможности бесплатного получения какой-то вещи, не вводите пароли, номера телефонов, кредитных карт или другую личную информацию без обсуждения этой ситуации с родителями.

· В сети существует масса возможностей для скачивания программного обеспечения, музыки, игр, документов и т. д. При этом многие из них содержат вирусы. Поговорите со своими родителями, прежде чем загружать такие ресурсы. Не открывайте вложение, полученное от того, кого вы не знаете.

Правила информационной безопасности для школьников:

· Если вы получили по Интернету оскорбительное или иное сообщение, заставляющее вас чувствовать себя некомфортно, не отвечайте на него; обязательно расскажите об этом своим родителям или учителю в школе.

· Онлайн-друг может быть совсем не тем человеком, за кого он себя выдает. Не соглашайтесь на встречу с онлайн-другом без одобрения ваших родителей.

Основные правила по личному пространству

https://resh.edu.ru/subject/lesson/3049/main/

Проверка осознанности!

Денис установил программу, которая обеспечивает текстовую, голосовую и видеосвязь через Интернет. Как правильно вести себя Денису в общении со знакомыми с помощью этой программы?

Если используете видеокамеру, то приведите себя и комнату в порядок.

Если разговор надоел, то можно отключить программу, потом сказать, что были технические проблемы у провайдера.

Если адресат не отвечает сразу, то надо исключить его из списка контактов.

Вежливо обращаться к собеседникам, не перебивать, уважать чужое мнение.

Иван модифицируете свой компьютер и устанавливает повторно купленное им ранее программное обеспечение. Количество кодов активации закончилось. В лицензионном соглашении указано: «Лицензия на использование программного обеспечения выдаётся отдельно на каждого пользователя. Процедура активации связывает использование программного обеспечения с конкретным устройством. Если Вы измените компоненты компьютера или внесете изменения в программное обеспечение, то может потребоваться повторная активация.»
Какие действия считаются правомерными?

Активировать с помощью любого скачанного из интернета кода.

Воспользоваться кодом активации, позаимствованным у своего товарища.

Обратиться в лицензионный отдел фирмы изготовителя и получить ключ активации по телефону.

Оплатить дополнительный ключ активации, заполнив запрос на сайте производителя.

Дмитрий получил письмо по электронной почте с адреса priz2015@mymail.abc:

Уважаемый клиент!

Поздравляем, номер вашего заказа при покупке товаров в интернет-магазине стал победителем лотереи. Перейдите по ссылке priz2015.abc и оформите получение приза.

Какой вариант поведения в этой ситуации более безопасный?

- Перейти по ссылке в письме, чтобы получить подарок.
- Заблокировать получение писем от этого отправителя.
- Написать ответное письмо, о том, что не участвовал в лотерее.
- Переслать письмо другу.

Что следует предпринять, если вы получили по Интернету оскорбительное или иное сообщение, заставляющее вас чувствовать себя некомфортно?

- ✓ Сообщить учителю.
- Ответить на письмо.
- ✓ Сообщить родителям.
- Сообщить друзьям.
- ✓ Не отвечать на письмо.

Свой пароль можно сообщить:

родителям

друзьям

всем желающим

Какую информацию о себе можно разместить в открытом доступе в Интернете?

Номер телефона.

Фамилию.

Место работы родителей.

О прочитанных книгах.

Когда можно полностью доверять новым онлайн-друзьям?

Ничто не может дать полную гарантию того, что онлайн-другу можно доверять.

Когда есть общие друзья.

После обмена фотографиями.

После длительного онлайн-знакомства (переписки).

Что предпочтительнее делать, если вы увидели на сайте сообщение о том, что одна из программ на вашем компьютере устарела и требует обновления?

Найти официальный сайт этой программы и скачать обновление оттуда.

Нажать на эту ссылку и перейти к скачиванию обновления.

Открыть программу, о которой идёт речь, найти в её меню обновления, и, при их наличии, обновиться через программу.