федеральное государственное автономное образовательное учреждение высшего образования

Первый Московский государственный медицинский университет им. И.М. Сеченова Министерства здравоохранения Российской Федерации

(Сеченовский Университет)

Институт цифровой медицины

Кафедра информационных и интернет технологий

Методические материалы по дисциплине:

Информационные технологии

основная профессиональная образовательная программа высшего образования - программа специалитета

КОД Наименование ОП: 31.05.02 Педиатрия

Сеченовский Университет
наук о жизни

Практическое занятие. Защита персональных данных

Рябков И.В.

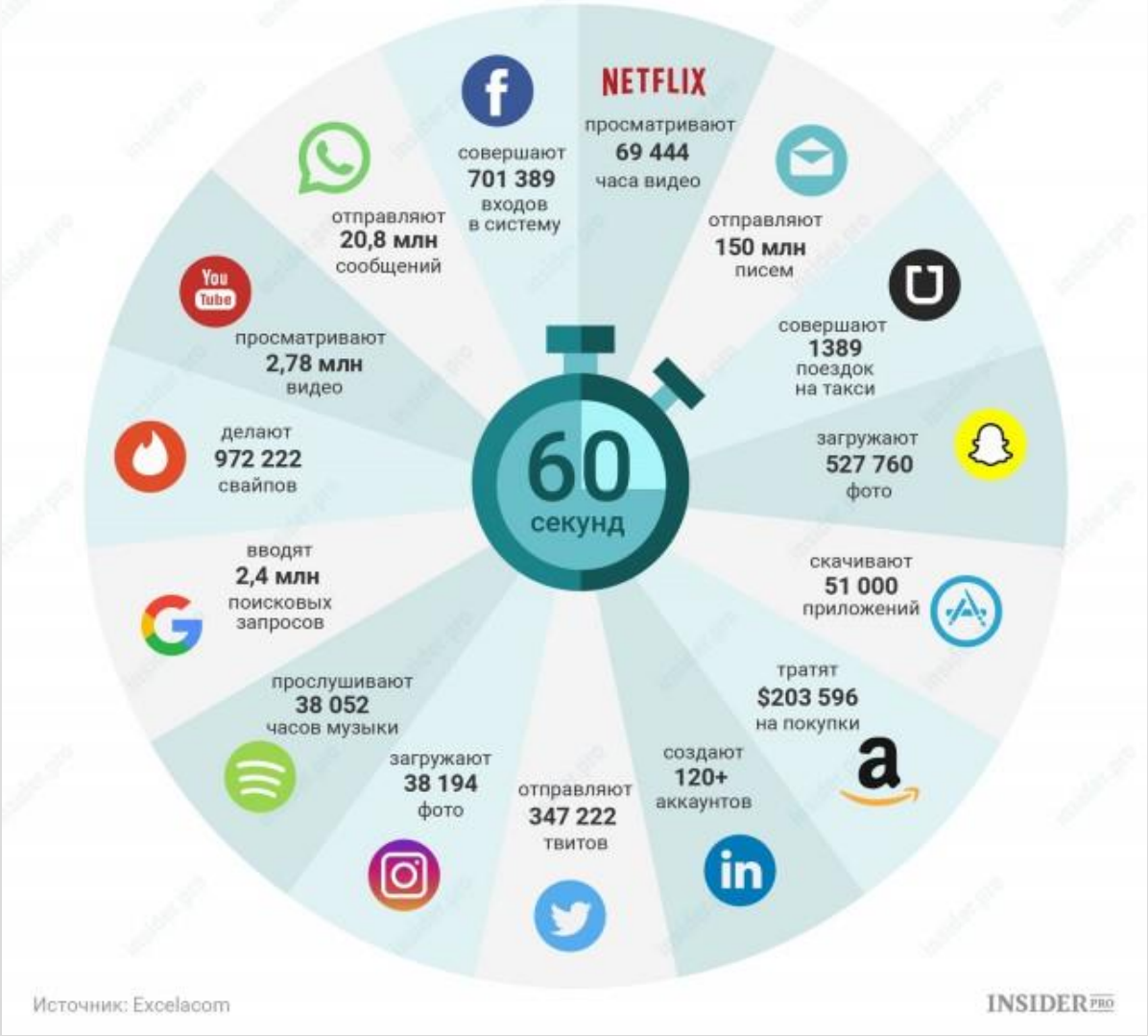
Три кита

Безопасность начинается в нашей голове.

От безопасности до безумия один шаг.

Ощущение безопасности самая опасная иллюзия

Интернет неотъемлемая часть жизни



Сеченовский Университет
наук о жизни

Кражи века

145 миллионов записей с информацией о дате рождения, почтовыми адресами были скомпрометированы

56 миллионов записей о дебетовых и кредитных картах были украдены

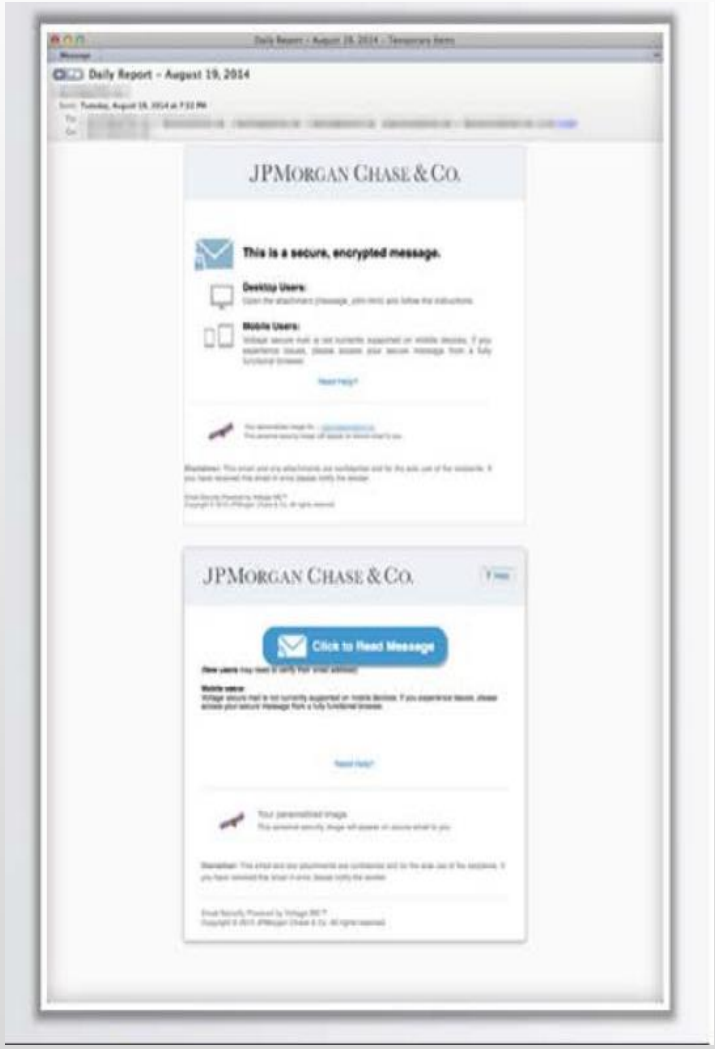
22 сентября 2016 года компания признала факт кражи данных не менее 500 миллионов аккаунто

JPMorgan обокрали

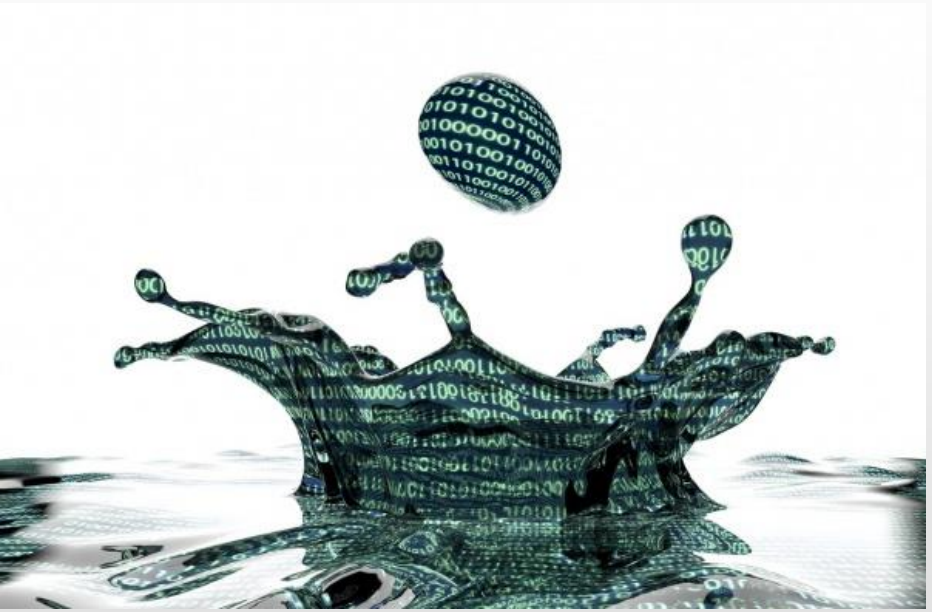
Contact information for **76 million households** and **7 million small businesses** were compromised

Incident occurred due to **attack on web applications**

JPMorganChase



Данные 119 тыс. клиентов FedEx обнаружены в открытом доступе в Сети



Отсканированные копии паспортов, водительских удостоверений и другой документации 119 тыс. клиентов службы доставки FedEx оказались в открытом доступе в Сети из-за некорректно настроенного сервера Amazon

Удостоверения личности были прикреплены к формам, содержащим персональные данные клиентов, такие как имена, домашние адреса, номера телефонов и почтовые индексы

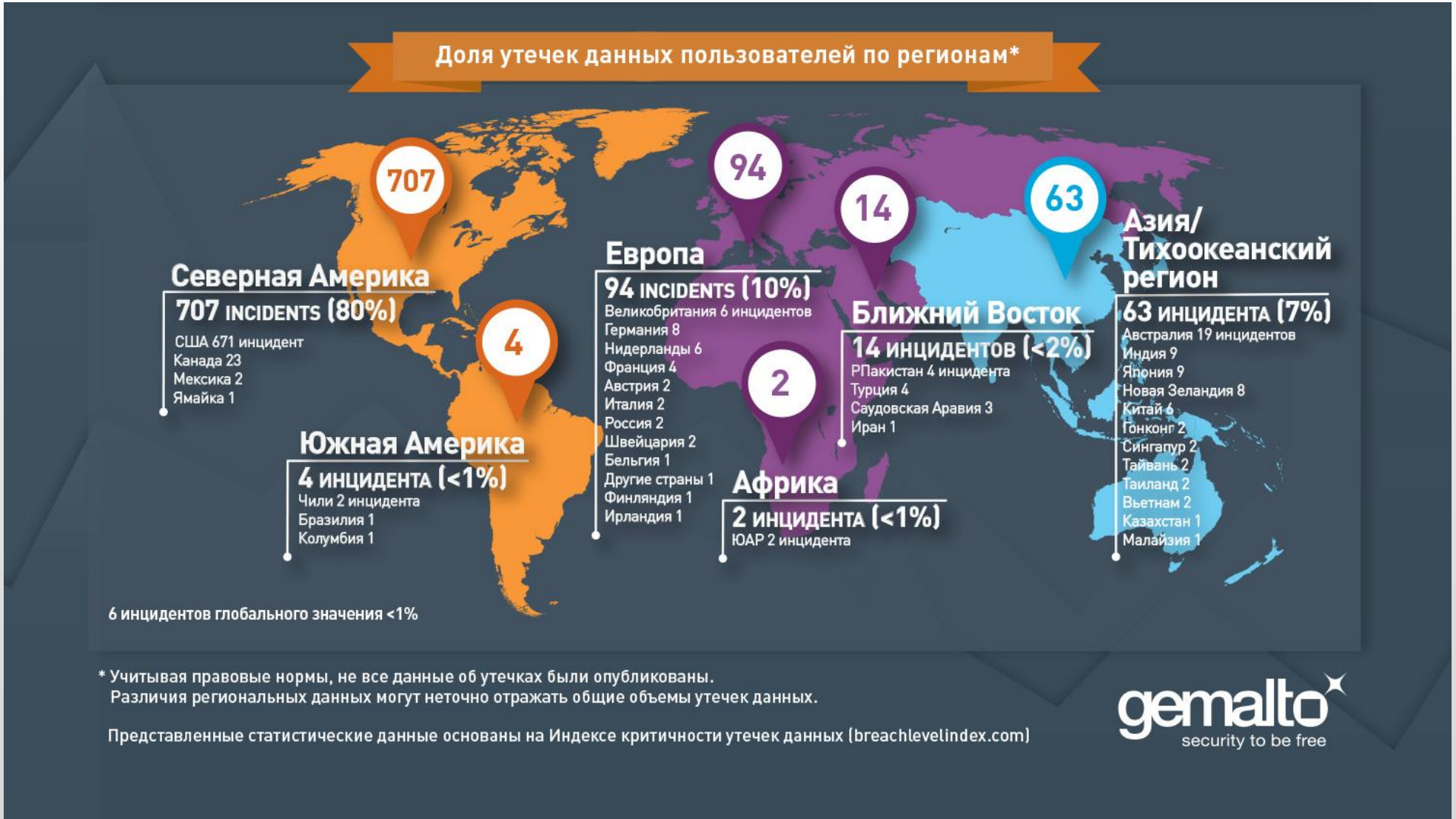
Отсканированные копии документов принадлежали клиентам из стран по всему миру, в том числе из США, Мексики, Канады, Австралии, Саудовской Аравии, Японии, Китая и

SWISSCOM и Infraud

Персональная информация 800 тыс. абонентов швейцарского оператора связи Swisscom оказалась скомпрометирована в результате взлома систем оператора. В руках злоумышленников оказались имена, даты рождения, адреса и номера телефонов клиентов Swisscom.

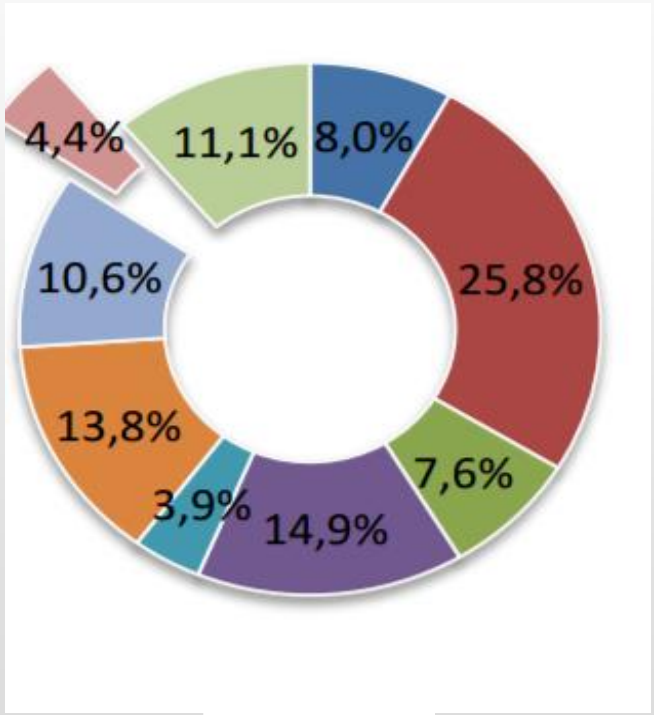
7 февраля, Министерство юстиции США сообщило о пресечении деятельности международной киберпреступной группировки, осуществлявшей незаконную деятельность на организованной ими подпольной интернет-площадке Infraud. Злоумышленники разработали сложную схему по покупке и продаже номеров социального страхования, данных о днях рождения и паролях, похищенных у пользователей со всего мира. Ущерб от деятельности кибергруппы оценивается в **$530 млн**. В общей сложности ведомство предъявило очные и заочные обвинения 36 участникам группировки, в том числе

Доля утечек данных пользователей



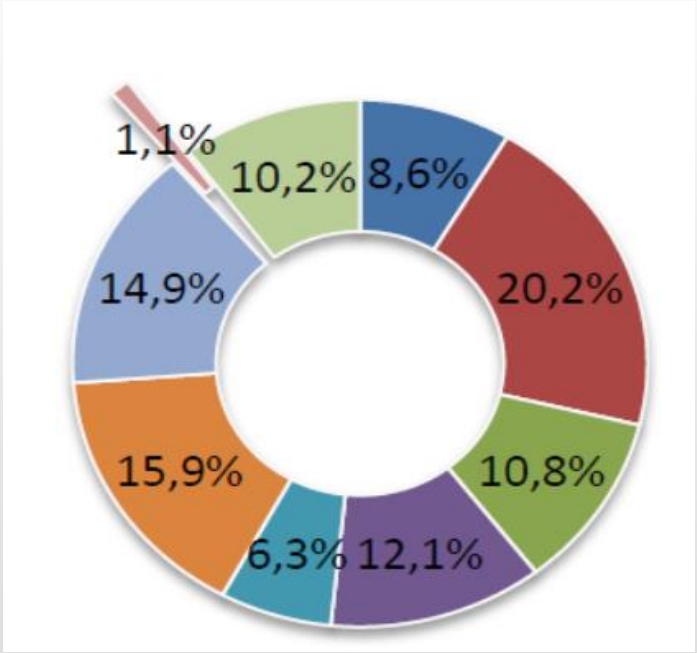
Утечка данных

Распределение числа утечек и объема скомпрометированных персональных данных по отраслям от InfoWatch.



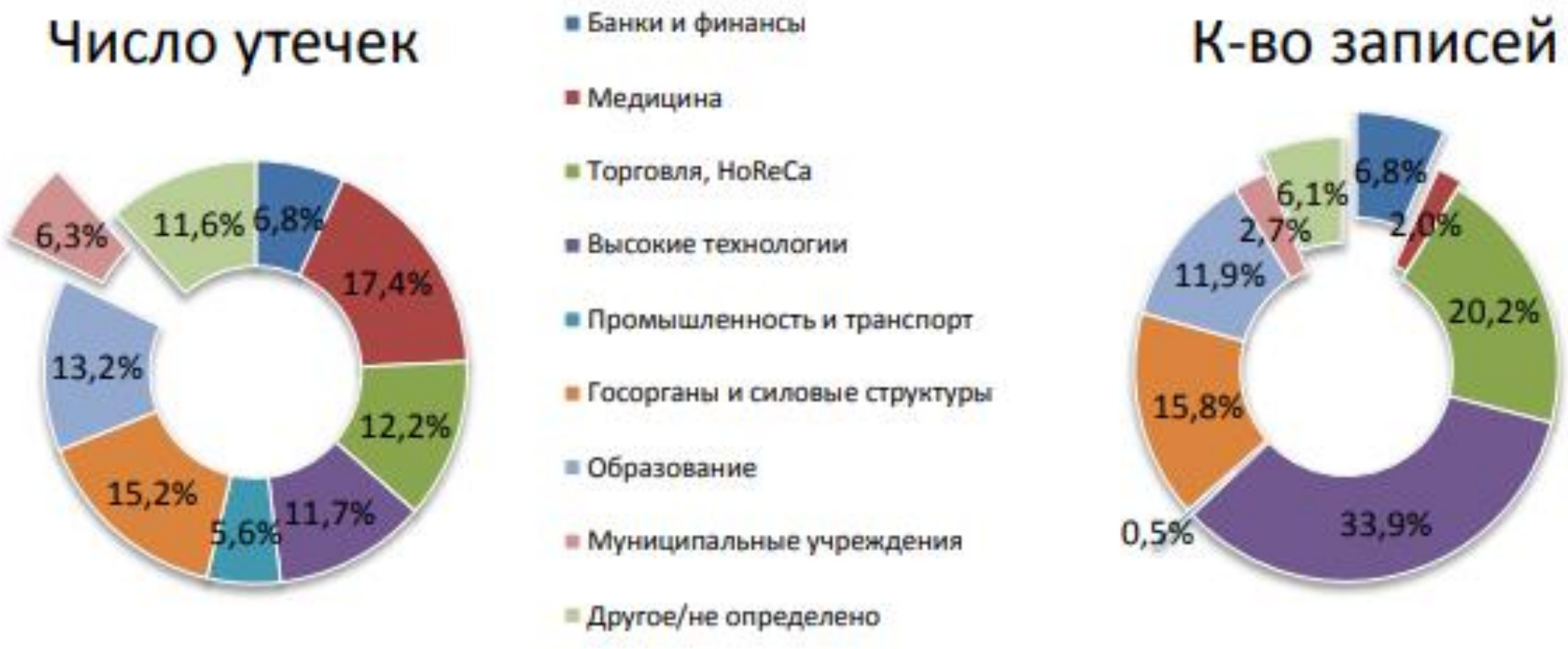
2016 г.

- Банки и финансы
- Медицина
- Торговля, HoReCa
- Высокие технологии
- Промышленность и транспорт
- Госорганы и силовые структуры
- Образование
- Муниципальные учреждения
- Другое/не определено



2015 г.

Распределение числа утечек и объема скомпрометированных персональных данных по отраслям от InfoWatch (первое полугодие 2017г).



Преступления и наказания в интернете

Сеченовский Университет
наук о жизни

Погружение в Dark Web: куда уходят данные?

Специалисты в области безопасности из компании Bitglass решили провести эксперимент и выяснить, куда попадают украденные данные. Excel-файл с 1568 поддельными записими несуществующих сотрудников компании разместили на один из файлообменников The Dark Web. Файл оснастили небольшим «сюрпризом» — специальной ватермаркой, которая помогает специалистам определить место, где открывали документ — географическую локацию, IP-адрес и тип устройства. Специалисты отметили, что эту ватермарку невозможно удалить, а при копировании данных из этого файла в другой она также помечает копию.

Результаты эксперимента

Несколько дней спустя команда получила информацию о том, что поддельные записи скачали в 5 странах на 2 континентах и просмотрели 200 раз. На 12 день файл получил 1080 кликов и

Сеченовский Университет
наук о жизни

ПерсДанные = $$$$$$

= 4$

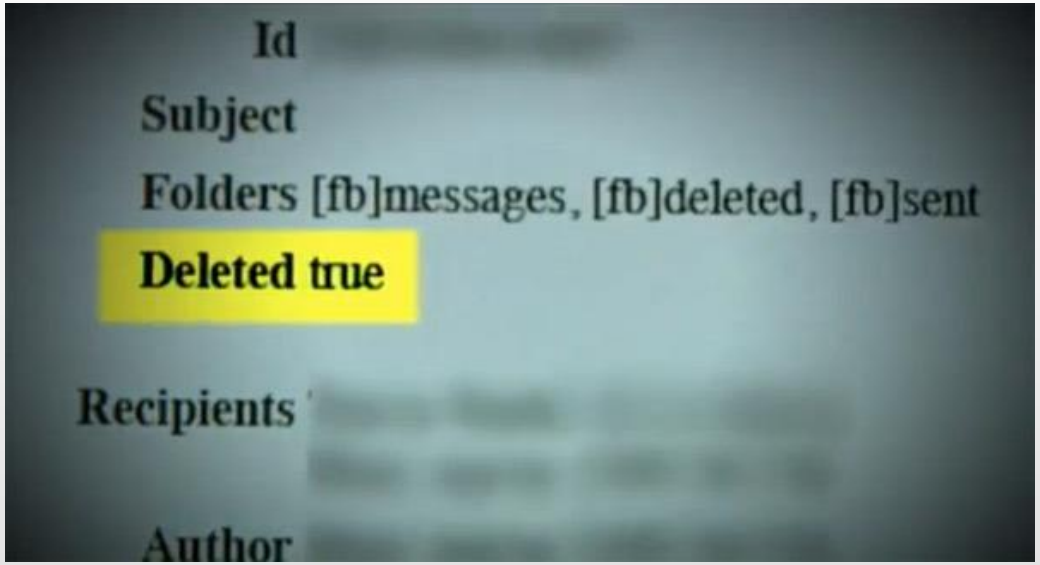
= 24$

Наши персональные данные можно приравнять к валюте , в обмен на котору
мы получаем определенные продукты, услуги, сервисы.

Компании получают информацию, перепродают ее другим.

24-летний студент начал войну против Facebook

Сеченовский Университет
наук о жизни



Макс Шремс

В результате длительных переговоров он получил по почте CD, содержащий PDF-файл на 1 222 страницы, на которых содержалась информация о его трудоустройстве, отношениях с окружающими, деталях личной жизни, старая переписка и фотографии с координатами мест, где они были сняты. Там были даже те фотографии которые он собственноручно удалил из профайла.

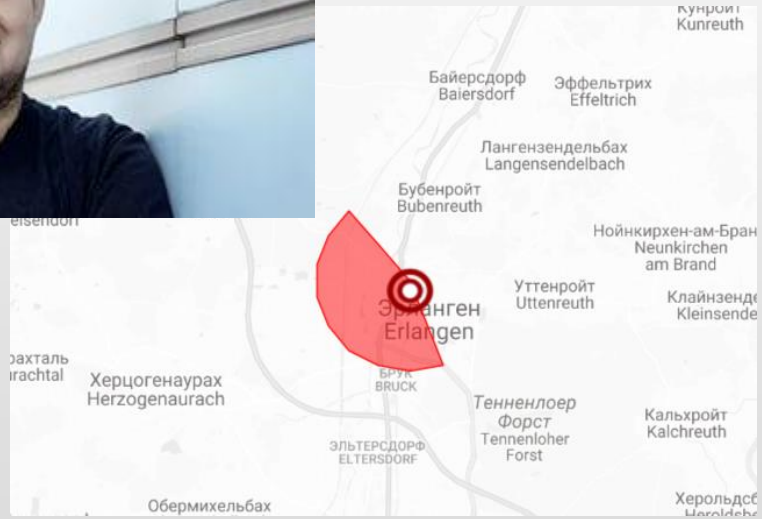
В Германии суд обвинил Facebook в незаконном использовании Пдн

«Facebook скрывает настройки по умолчанию и не предоставляет пользователям достаточной информации об использовании их данных при регистрации […] Это не соответствует определению информированного согласия», - заявили правозащитники

Одна из проблем заключалась в том, что в приложении Facebook для смартфонов была по умолчанию активирована услуга отображения местоположения пользователя его собеседнику.

Помимо этого, в настройках конфиденциальности были по умолчанию активированы функции, позволяющие поисковым системам ссылаться на временную шкалу пользователя, позволяя быстро и легко найти профиль конкретного пользователя

Мальте Шпитц und Deutsche Telecom

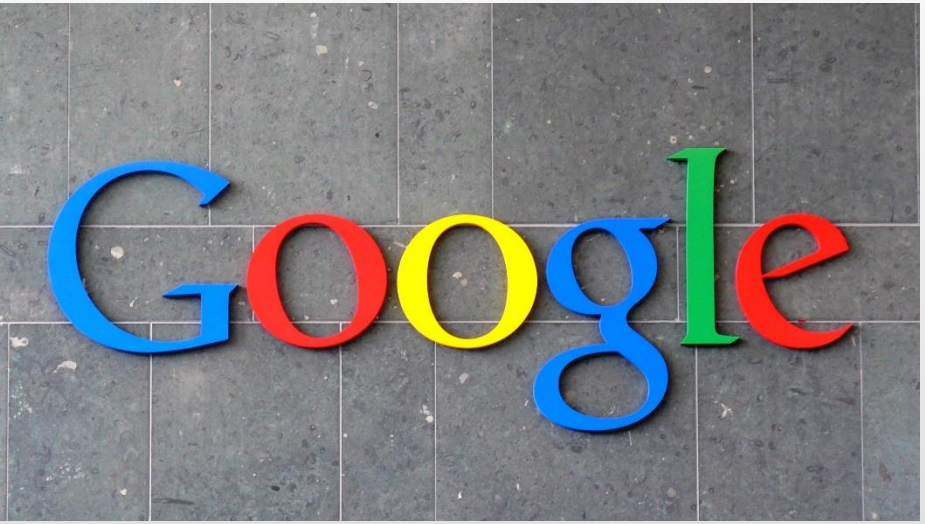


Он также получил CD, в котором был файл длиной в 36 000 строк, а затем обнародовал их. Сотрудники газеты Die Zeit помогли сопоставить метаданные с информацией о Шпитце из открытых источников.

Информация, собранная провайдером, поражает своей глубиной и уровнем детализации. Можно узнать, в какой день Шпитц ездил за город, где и во сколько обедал, с кем разговаривал.

Смонтированный журналистами интерактивный ролик размещён на сайте газеты Die Zeit

Google записывает и прослушивает



Компания Google никогда не скрывала того факта, что она собирает любую доступную информацию о пользователях и тщательно её сберегает.

- поисковые запросы и просмотренные страницы;
- места, которые вы посетили;
- информация с устройств;
- **голосовые запросы и команды;**
- видео, которые вы искали на YouTube;
- видео, которые вы смотрели на YouTube.

Калькулятор стоимости собственных данных

Сколько ты стоишь
http://www.ft.com/

Стоимость личности

Сеченовский Университет
наук о жизни

Hacker Products and Services	Price in 2013	Price in 2014
Visa and Master Card (US)	$4	$4
American Express (US)	$7	$6
Discover Card with (US)	$8	$6
Visa and Master Card (UK, Australia and Canada)	$7 -$8	$8
American Express (UK, Australia and Canada)	$12- $13	$15(UK and Australia); $12 (CA)
Discover Card (Australia and Canada)	$12	$15(Australia); $10(CA)
Visa and Master Card (EU and Asia)	$15	$18-$20
Discover and American Express Card (EU and Asia)	$18	$18-$20
Credit Card with Track I and II Data (US)	$12	$12
Credit Card with Track I and II Data (UK, Australia and Canada)	$19-$20	$19-$20
Credit Card with Track I and II Data (EU, Asia)	$28	$28
US Fullz	$25	$30

Скан карточки соц. страхования США вместе с именем и фамилией стоит $250, дополнительные документы к ним (счета по кредиткам, и т.п.) – ещё $100. Поддельные водительские права идут всего по $100-150. В сумме, чтобы «украсть», как говорят, личность и получить доступ к медицинскому обслуживанию, программам гос. помощи или получить кредит, потребуется чуть меньше $500.

Продай свои данные

A bite of Me
https://www.kickstarter.com/
Продает свои данные.

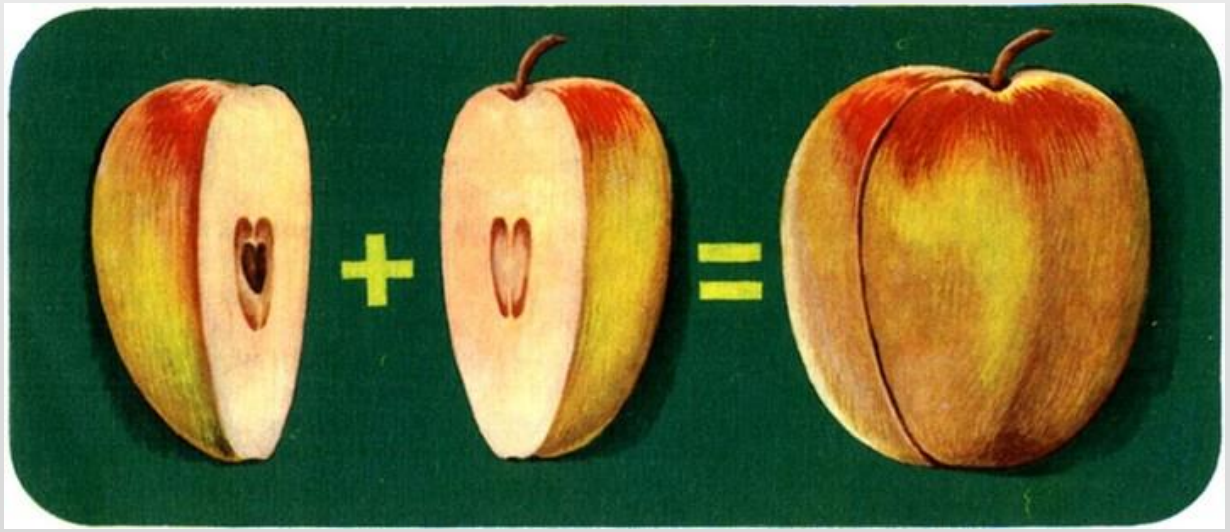
Handshake
http://www.handshake.uk.com/
Доход от 1000$ до 5000$

Datacoup
https://datacoup.com/
Ежемесячно 8$ за данные

Информационная безопасность

Сеченовский Университет
наук о жизни

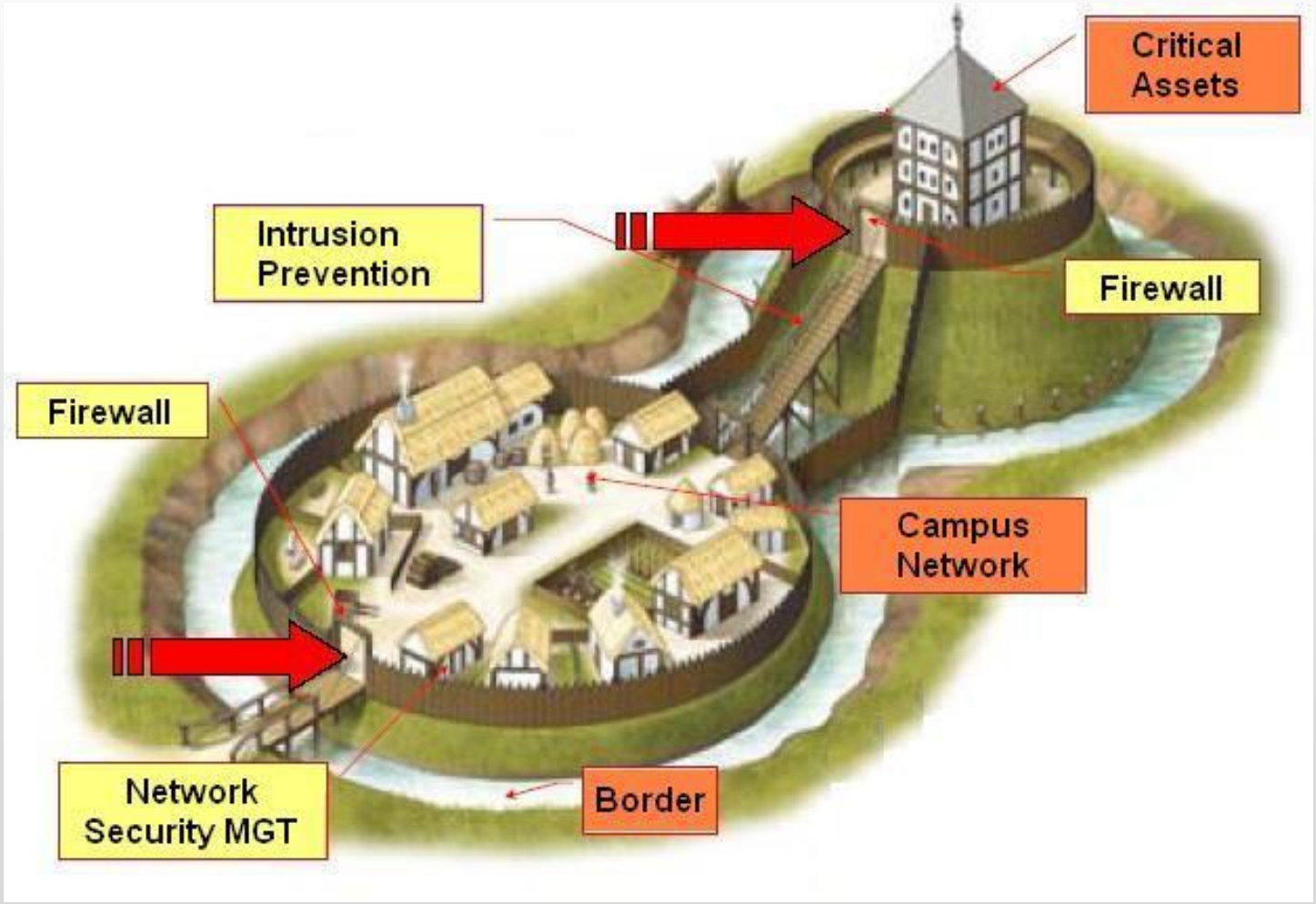
Информационная безопасность - комплекс организационных, технических мер по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе.



Уровни информационной безопасности

У каждого свои задачи, свои подходы, свои мероприятия. И часто они конфликтуют между собой.

Модель DEFENSE IN DEPTH
Глубокоэшелонированная защита



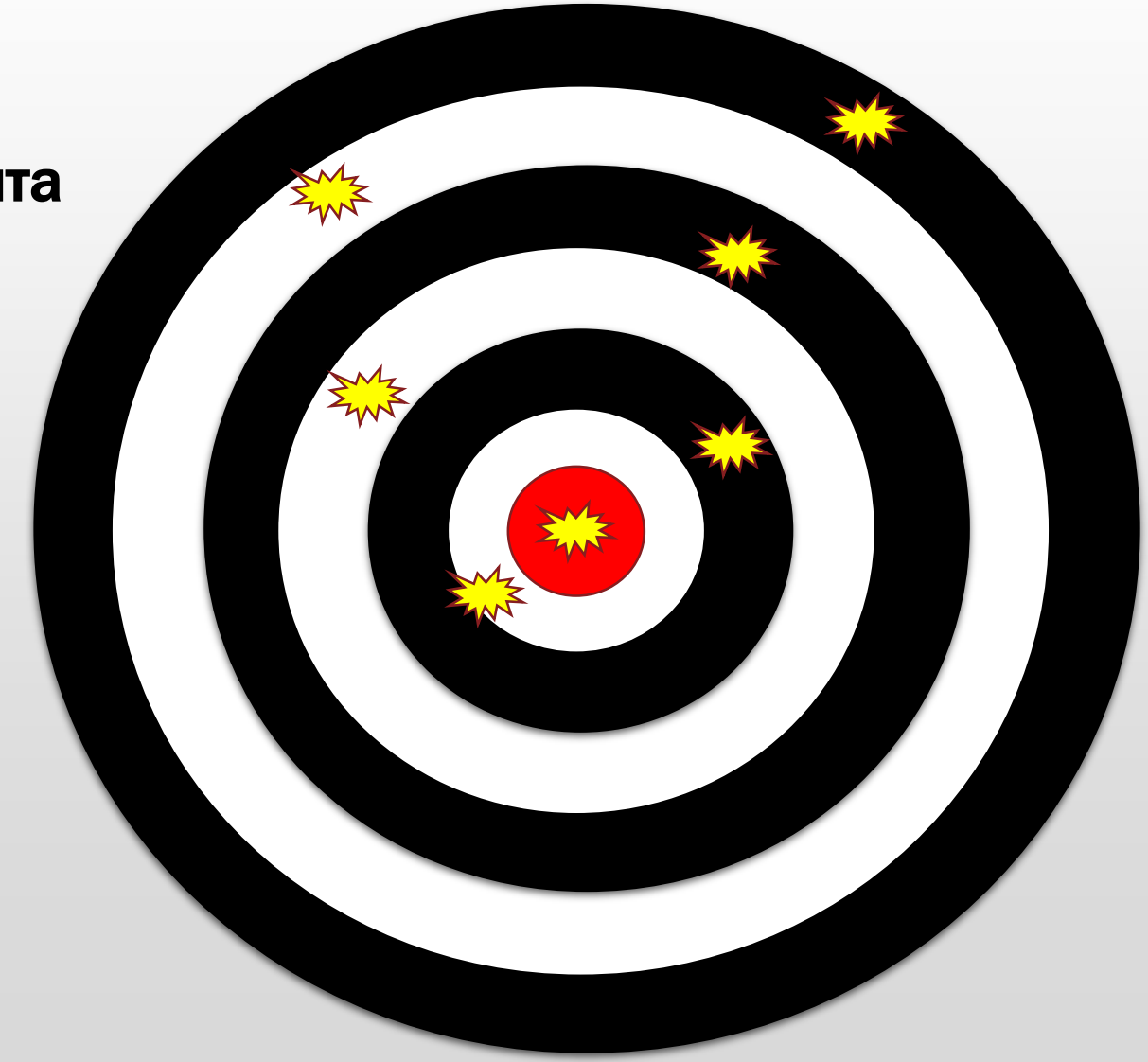
DEFENSE IN DEPTH
Глубокоэшелонированная защита

Сеченовский Университет
наук о жизни

Физическая защита

Внутренняя сеть

Приложение



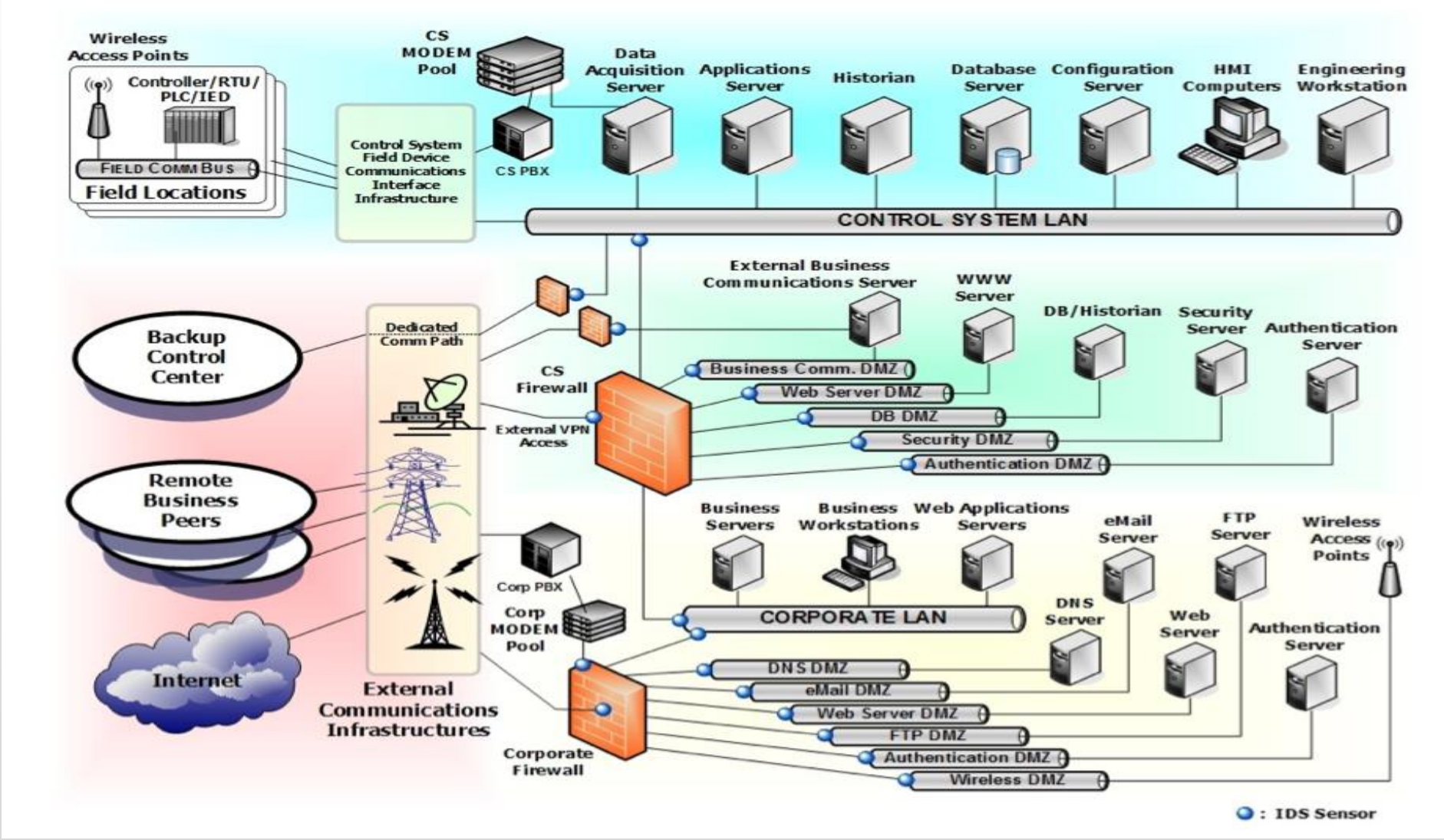
Закон / полиция

Периметр организации

Сервер / Компьютер

Информация / Данные

DEFENSE IN DEPTH
Глубокоэшелонированная защита



Основные виды информационных угроз

Угроза «информационной безопасности» – это потенциальная возможность нарушения режима

Основные принципы построения системы информационной безопасности

- Законность
- Системность
- Комплексность
- Непрерывность
- Своевременность
- Преемственность и непрерывность совершенствования
- Разумная достаточность
- Персональная ответственность
- Разделение функций
- Минимизация полномочий
- Взаимодействие и сотрудничество
- Гибкость системы защиты
- Простота применения средств защиты

Основные виды несанкционированного воздействия на информацию

- Модификация
- Уничтожение
- Искажение
- Подделка
- Блокировка доступа
- Хищение носителя

Виды нарушителей информационной безопасности

Нарушитель – лицо, предпринявшее попытку выполнения запрещенных операций по ошибке, незнанию или осознано со злым умыслом(из корыстных интересов, или без такового и использующие для этого различные возможности, методы и средства

- Внутренние (пользователи, персонал, руководители различных уровней)

- Внешние (Внешние разработчики, конкуренты, клиенты, технический персонал)

Система нормативно-правовых актов по защите персональных данных

Сеченовский Университет
наук о жизни

Конвенция о защите физических лиц при автоматизированной обработке персональных данных(Страсбург, 28 января 1981 г.)

Конституция РФ

Федеральный закон от 19 декабря 2005 г. **№ 160-ФЗ** «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

Система нормативно-правовых актов по защите персональных данных

Сеченовский Университет
наук о жизни

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

ПП РФ от 01 ноября 2012 **№ 1119**

ПП РФ от 15 сентября 2008 **№ 687**

ПП РФ от 06 июля 2008 **№ 512**

ПП РФ от 03 ноября 1994 № 1233

ПП РФ от 4 марта 2010 г. N 125 "

ПП РФ от 21 марта 2012 года **№ 211**

Приказ Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»

Приказ ФСТЭК, ФСБ, Мининформсвязи от 13 декабря 2013 № 151/786/461

Приказ ФСТЭК РФ от 18 февраля 2013г. № 21

Приказ ФСБ РФ от 09 февраля 2005 № 66

Методические документы ФСБ

Методические документы ФСТЭК

Указ Президента РФ от 06 марта 1997 № 188 «Об утверждении перечня сведений конфиденциального характера»

Указ Президента РФ от 30 мая 2005 г. **№ 609** «Об утверждении Положения о персональных данных государственного гражданского служащего РФ и ведении его личного дела»

Указ Президента РФ от 17 марта 2008 **№ 351** «О мерах по обеспечению информационной безопасности РФ при использовании информационно-телекоммуникационных сетей международного информационного обмена»

Трудовой кодекс РФ «Защита персональных данных работника»

ФЗ закон от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Государственные стандарты

- ГОСТ Р 51275-2006. «Объект информации. Факторы, воздействующие на информацию. Общие положения»;
- ГОСТ 34.003-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения»;
- ГОСТ 34.201-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании информационных систем»;
- ГОСТ 34.601-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы.. Стадии создания»;
- ГОСТ 34.602-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;
- ГОСТ Р 51624-2000. «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования»;
- ГОСТ Р 50922-2006. «Защита информации. Основные термины и определения»;
- ГОСТ Р 53114-2008. «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения»;
- ГОСТ Р ИСО/МЭК 15408-1-2008. «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель»;
- ГОСТ Р 51583-2014. «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

Контролирующие органы в области защиты персональных данных

Сеченовский Университет
наук о жизни

Роскомнадзор

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций

Орган по защите прав субъектов Пдн

ФСТЭК

Федеральная служба по техническому и экспортному контролю

Федеральный орган, уполномоченный в области противодействия техническим разведкам и технической защиты информации

ФСБ

Федеральная служба безопасности

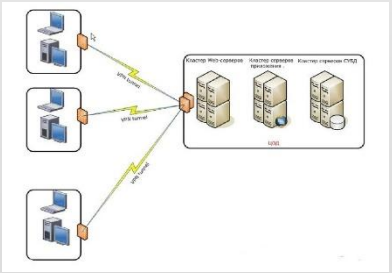
Федеральный орган, уполномоченный в области обеспечения безопасности

Роструд

Федеральная служба по труду и занятости

Федеральный орган, по контролю и надзору за соблюдением трудового законодательства и иных нормативных правовых актов, содержащих нормы трудового права

Основные определения и сокращение ФЗ - 152



Персональные данные(ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

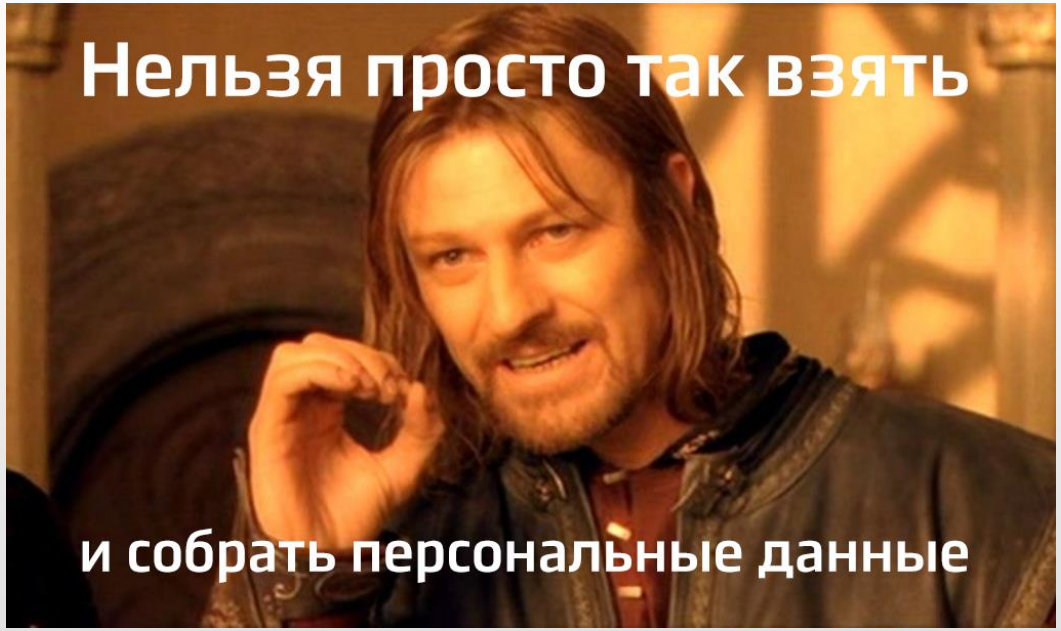
Оператор - государственный орган или муниципальный орган, юридическое или физическое лицо, осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

ИСПД (ИСПДн) - информационная система Пдн (совокупность Пдн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких Пдн с использованием средств автоматизации или без использования таких средств)

Обработка Пдн - любое действие (операция), совершаемых с использованием средств автоматизации или без использования таких средств с Пдн

Основа основ
ПДн *базируется на принципах законности и справедливости*

Сеченовский Университет
наук о жизни



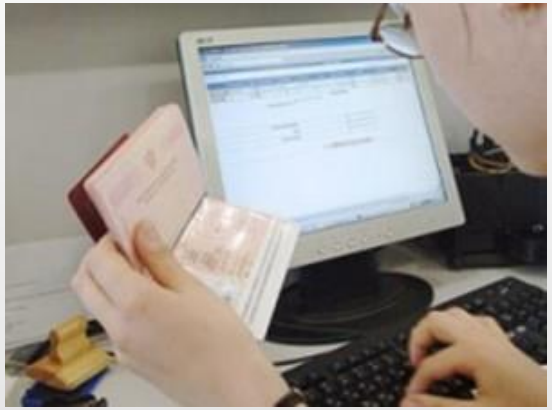
- **Обработка персональных данных должна отвечать целям сбора персональных данных;**
- **Не должны объединяться базы данных, содержащих персональные данные, обработка которых осуществляется в несовместимых между собой целях;**
- **Обрабатываемый объем персональных данных не должен быть избыточным по отношению к целям их обработки;**
- **При обработке персональных данных должны быть обеспечены их точность, достаточность и актуальность по отношению к целям обработки;**
- **Хранение персональных данных должно осуществляться не дольше, чем этого требуют цели обработки персональных данных.**

Этапы работы с персональными данными

Сеченовский Университет
наук о жизни

Сбор

Использование



Уничтожение

Хранение

Блокирование

Передача

ПП РФ от 01 ноября 2012 № 1119

Постановление Правительства Российской Федерации от 01 ноября 2012 № 1119«Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

- Определяются типы актуальных угроз.
- Устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных и уровни защищенности таких данных.

- При обработке персональных данных в информационных системах устанавливает 4 уровня защищенности персональных данных.

- Определяет ответственное лицо, кто должен обеспечить защиту данных, при обработке в информационных системах.

Виды информационных систем ПДн

(ПП РФ от 01 ноября 2012 № 1119)

Сеченовский Университет
наук о жизни

Типы актуальных угроз
(ПП РФ от 01 ноября 2012 № 1119)

Сеченовский Университет
наук о жизни

- 1-го типа.Связаны с наличием НДВ в системном ПО
- 2-го типа.Связаны с наличием НДВ в прикладном ПО
- 3-го типа.Не связаны с наличием НДВ в системном и прикладном ПО

Уровни защищенности
(ПП РФ от 01 ноября 2012 № 1119)

Сеченовский Университет
наук о жизни

В зависимости от уровня защищенности ПДн определяется перечень требований, выполнение которых необходимо для нейтрализации угроз безопасности персональных данных.

Категории ПДн		Специальные			Биомет-рические	Иные			Общедоступные		
Собственные работники		нет	нет	да		нет	нет	да	нет	нет	да
Количество субъектов		более 100 тыс.	менее 100 тыс.			более 100 тыс.	менее 100 тыс.		более 100 тыс.	менее 100 тыс.	
Тип актуальных угроз	1	1 УЗ	1 УЗ	1 УЗ	1 УЗ	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ
	2	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	3 УЗ	3 УЗ	2 УЗ	3 УЗ	3 УЗ
	3	2 УЗ	3 УЗ	3 УЗ	3 УЗ	3 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ

Информационная безопасность. Виды ответственности.

Сеченовский Университет
наук о жизни

Гражданская ответственность

Дисциплинарная ответственность

Административная ответственность

Уголовная ответственность

Гражданская ответственность за несоблюдение законодательства

Статья 15 Федерального закона №152-ФЗ

Субъект ПДн имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и компенсацию морального вреда в судебном порядке.

Статья 24 Федерального закона №152-ФЗ

Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки ПДн, а также требований к защите ПДн, установленных законодательством о персональных данных, подлежит возмещению. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом убытков.

Дисциплинарная ответственность за несоблюдение законодательства

Подпункт "в" п. 6 ч. 1 ст. 81 Трудового кодекса

Разглашение одним работником персональных данных другого, если они стали известны ему в связи с исполнением трудовых обязанностей. Увольнение

Статья 90, ст. 192 ТК РФ

Иные нарушения в области персональных данных при их обработке. Замечание или выговор

Административная ответственность за несоблюдение законодательства до 1 июля 2017г.

Статья 13.11 Кодекса РФ об административных правонарушениях

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет наказание в виде административного штрафа для юридических лиц от 5 до 10 тысяч рублей.

Статья 13.12 Кодекса РФ об административных правонарушениях

Использование несертифицированных средств защиты информации, в случае их обязательной сертификации, влечет наложение административного штрафа на юридических лиц от 10 до 20 тысяч рублей с конфискацией или без конфискации несертифицированных средств защиты информации.

Административная ответственность за несоблюдение законодательства после 1 июля 2017г.

Сеченовский Университет
наук о жизни

Статья 5.39 КоАП Неправомерный отказ в предоставлении гражданину и (или) организации информации, предоставление которой предусмотрено законом, несвоевременное ее предоставление либо предоставление заведомо недостоверной информации **Административный штраф на должностных лиц в размере от 5 тыс. до 10 тыс. руб**

Часть 1 ст. 13.11 КоАП РФ Обработка персональных данных в случаях, не предусмотренных законом, либо обработка, несовместимая с целями сбора персональных данных . **Предупреждение или административный штраф на граждан – от 1 тыс. до 3 тыс. руб.;на должностных лиц – от 5 тыс. до 10 тыс. руб.;на юридических лиц – от 30 тыс. до 50 тыс. руб.**

Часть 2 ст. 13.11 КоАП РФ Обработка персональных данных без письменного согласия субъекта, когда это необходимо, либо обработка данных с нарушением требований к составу сведений, включаемых в такое согласие. **Предупреждение или административный штраф – на граждан – от 3 тыс. до 5 тыс. руб.; на должностных лиц – от 10 тыс. до 20 тыс. руб.;на юридических лиц – от 15 тыс. до 75 тыс. руб.**

Часть 3 ст. 13.11 КоАП РФ Невыполнение оператором обязанности по опубликованию или обеспечению иным образом неограниченного доступа к политике обработки персональных данных **Предупреждение или административный штраф: на граждан – от 700 до 1 тыс. руб.; на должностных лиц – от 3 тыс. до 6 тыс.**

Административная ответственность за несоблюдение законодательства после 1 июля 2017г.

Сеченовский Университет
наук о жизни

Часть 4 ст. 13.11 КоАП РФ Невыполнение оператором обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных. **Предупреждение или административный штраф: на граждан – от 1 тыс. до 2 тыс. руб.; на должностных лиц – от 4 тыс. до 6 тыс. руб.; на индивидуальных предпринимателей – от 10 тыс. до 15 тыс. руб.; на юридических лиц – от 20 тыс. до 40 тыс. руб**

Часть 5 ст. 13.11 КоАП РФ Невыполнение оператором в установленные сроки требования субъекта персональных данных или его представителя либо Роскомнадзора об уточнении персональных данных, их блокировании или уничтожении (если данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки) **Предупреждение или административный штраф: на граждан – от 1 тыс. до 2 тыс. руб.; на должностных лиц – от 4 тыс. до 10 тыс. руб.; на индивидуальных предпринимателей – от 10 тыс. до 20 тыс. руб.; на юридических лиц – от 25 тыс. до 45 тыс. руб.**

Часть 6 ст. 13.11 КоАП РФ Невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих их сохранность и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении них**. Административный штраф: на граждан – от 700 до 2 тыс. руб.; на должностных лиц – от 4 тыс. до 10 тыс. руб.; на индивидуальных предпринимателей – от 10 тыс. до 20 тыс. руб.; на юридических лиц – от 25 тыс. до 50 тыс. руб.**

Часть 7 ст. 13.11 КоАП РФ Невыполнение оператором, являющимся государственным или муниципальным органом, обязанности по обезличиванию персональных данных либо несоблюдение установленных для этого требований или методов **Административный штраф: на граждан – от 700 до 2 тыс. руб.;на должностных лиц – от 4 тыс. до 10 тыс. руб.; на индивидуальных предпринимателей – от 10 тыс. до 20 тыс. руб.; на юридических лиц – от 25 тыс. до 50 тыс. руб.**

Уголовная ответственность за несоблюдение законодательства

Статья 137 Уголовного кодекса РФ. Нарушение неприкосновенности частной жизни

Максимальное наказание за данное преступление предусматривает лишение свободы нарушителя на срок до 4 лет

Статья 140. Отказ в предоставлении гражданину информации

Наказываются штрафом в размере до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет.

Статья 272. Неправомерный доступ к компьютерной информации

Наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

Судебная практика по ПДн

1. **Фамилия, имя, отчество, год, месяц, день и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия и паспорт**).

2. **Адрес электронной почты** (см., например, Решение по делу № 12-253/2015 от 26.05.2015. Калининский районный суд (город Санкт-Петербург). Роскомнадзор указывает, что адрес электронной почты, содержащий ФИО, будет отнесен к категории ПДн, а в случае если адрес представляет собой набор символов (слов), его нельзя считать персональными данными

3. **Адреса места жительства индивидуальных предпринимателей**, указанные в плане проведения проверок юридических лиц и индивидуальных предпринимателей, размещенном в общем доступе на официальном сайте администрации (см., например, Апелляционное определение Волгоградского областного суда от 24.04.2014 № 33-4427/2014).

4. **Сведения о пересечении государственной границы** (см., например, Апелляционное определение Московского городского суда от 10.04.2014 № 33-11688).

5. **Адрес регистрации должностного лица**, сведения о его доходах и собственности, распространяемые в непредусмотренной для официальной процедуры форме.

Тонкие материи
IP– адрес – Пдн или нет?

Помимо «простых» данных, вроде имени и фамилии, часто возникают вопросы относительно более «сложных» категорий типа IP-адреса, ника или профиля в социальной сети и их определения в качестве персональных данных.

В отнесении этих категорий персональных данных даже суды имеют разные точки зрения.

IP-адрес к ПДн не относят Постановление по делу № А56-75017/2014 от 01.06.2015. 13-й ААС), а другие, наоборот, признают (Решение по делу № А76-29008/2015 от 11.02.2016. АС Челябинской обл.).

Парадокс в следующем, что статичный IP-адрес справедливо относить к персональным данным, так как по нему идентифицировать пользователя легко. Но оператор не может знать, что будет являться статичным IP-адресом, в таком случае нужно признавать все IP адреса ПДн (на всякий пожарный).

Логин и пароль (от электронной почты или социальной сети) вызывает как раз меньше споров. Роскомнадзор неоднократно высказывался, что относить их к персональным данным нельзя.

Власти РФ отказались брать ответственность за утечки из ведомственных баз

Сеченовский Университет
наук о жизни

Российские власти ответили на запрос Европейского суда по правам человека (ЕСПЧ) касательно жалобы 46-летнего москвича, заявившего об утечке его персональных данных из базы ГУВД Москвы. **Как следует из ответа, государство не несет ответственности за утечки из ведомственных баз данных**

Согласно материалам дела, в 2011 году москвич обнаружил в открытом доступе базу данных ГУВД, в которой содержалась информация о том, что он является носителем ВИЧ-инфекции и был дважды судим.

Мужчина подал заявление в Следственный комитет с просьбой провести проверку по факту утечки, однако в ведомстве никак не отреагировали. Помимо этого, заявитель также пытался добиться проверки через суд или прокуратуру, однако безуспешно.

В 2012 году мужчина обратился в ЕСПЧ, в 2017 году суд коммуницировал данную жалобу и запросил у российских властей ответ, была ли у государства необходимость собирать такую информацию о гражданине и располагал ли он эффективными средствами защиты.

Права заявителя не нарушены, полиция имеет право обрабатывать данные о гражданах,


HOSPITAL

Медицинские организации

«Медучреждения вошли в тройку самых уязвимых с точки зрения утечек информации отраслей».

«На черном рынке стоимость медицинских сведений примерно в 10 раз выше цены за финансовую информацию (номера счетов, кредитных карт, проводки и так далее)».

Из громких инцидентов можно вспомнить историю лета 2014 года, когда сотрудник швейцарской скорой помощи пытался продать СМИ информацию из медицинской карты известного автогонщика Михаэля Шумахера за 50 тыс. евро.

Специальные категории

1. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частью 2 настоящей статьи.
2. Обработка указанных в части 1 настоящей статьи специальных категорий персональных данных допускается в случаях, если

4) обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

Криминальное использование персональных данных из поликлиники

Участились случаи когда после посещения медицинской организации и сдачи анализов в этот же день раздается звонок на домашний номер, представляются участковым терапевтом, главным врачом или сотрудником регистратуры.

После сообщают что исходя из полученных анализов ей поставили например диагноз «онкология» далее по ситуации пытаются навязать инновационное альтернативное **платное** лечение, либо получить дополнительную информацию о составе семьи и.т.д.

Факт - Преступники получили:

1.Доступ к личной информации - Знают ФИО и контактные данные.

2.Доступ к информации о посещение поликлиники - Звонок был в день посещения поликлиники и сдачи анализов.

Фарм-компании

В Вологодской области под видом представителя фармацевтической компании можно пройти в кабинет главного врача. Всего за 10 тысяч рублей он соглашается продавать персональные данные своих пациентов, причем на регулярной основе. Ни врачебная этика, ни возможное уголовное преследование руководителя больницы не останавливают. И кто будет пользоваться полученной информацией ему тоже, похоже, все равно

Основные нарушения и угрозы МИС

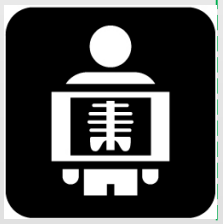
Информационная безопасность (ИБ) при функционировании МИС обеспечивается за счет взаимоувязанного комплексного использования оганизационных мер, программных и технических средств защиты.

Основные направления возможных нарушений ИБ:

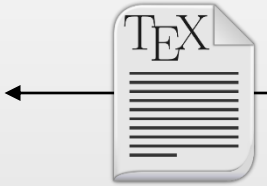
- утечка данных (нарушение конфиденциальности);
- утрата данных;
- несанкционированная модификация данных

- **Физический уровень** –– выведение из строя аппаратных средств хранения, обработки и передачи информации
- **Сетевой уровень** - блокирование работы серверов МИС, несанкционированный доступ к информационному ресурсу в результате ошибочных настроек
- **Уровень операционных систем** –– уничтожение прикладного ПО, нарушение правильной работы информационных серверов, клиентских рабочих мест в результате заражения компьютерным вирусом
- **Уровень управления БД-** наиболее опасной угрозой является НСД к БД в результате получения административных паролей СУБД

Обмен персональными данными



Контролируемая зона



Не контролируемая зона

Организационно-технических мероприятия по защите персональных данных в соответствии с ФЗ -152

ЭТАП I

- Инвентаризация всех информационных ресурсов и документации
- Разработка Модели Угроз
- Разработка и внедрение организационно-распорядительной документации

ЭТАП II

- Внедрение средств защиты информации
- Эксплуатации системы защиты ПДн
- Контроль эффективности системы защиты Пдн

Последовательность шагов по

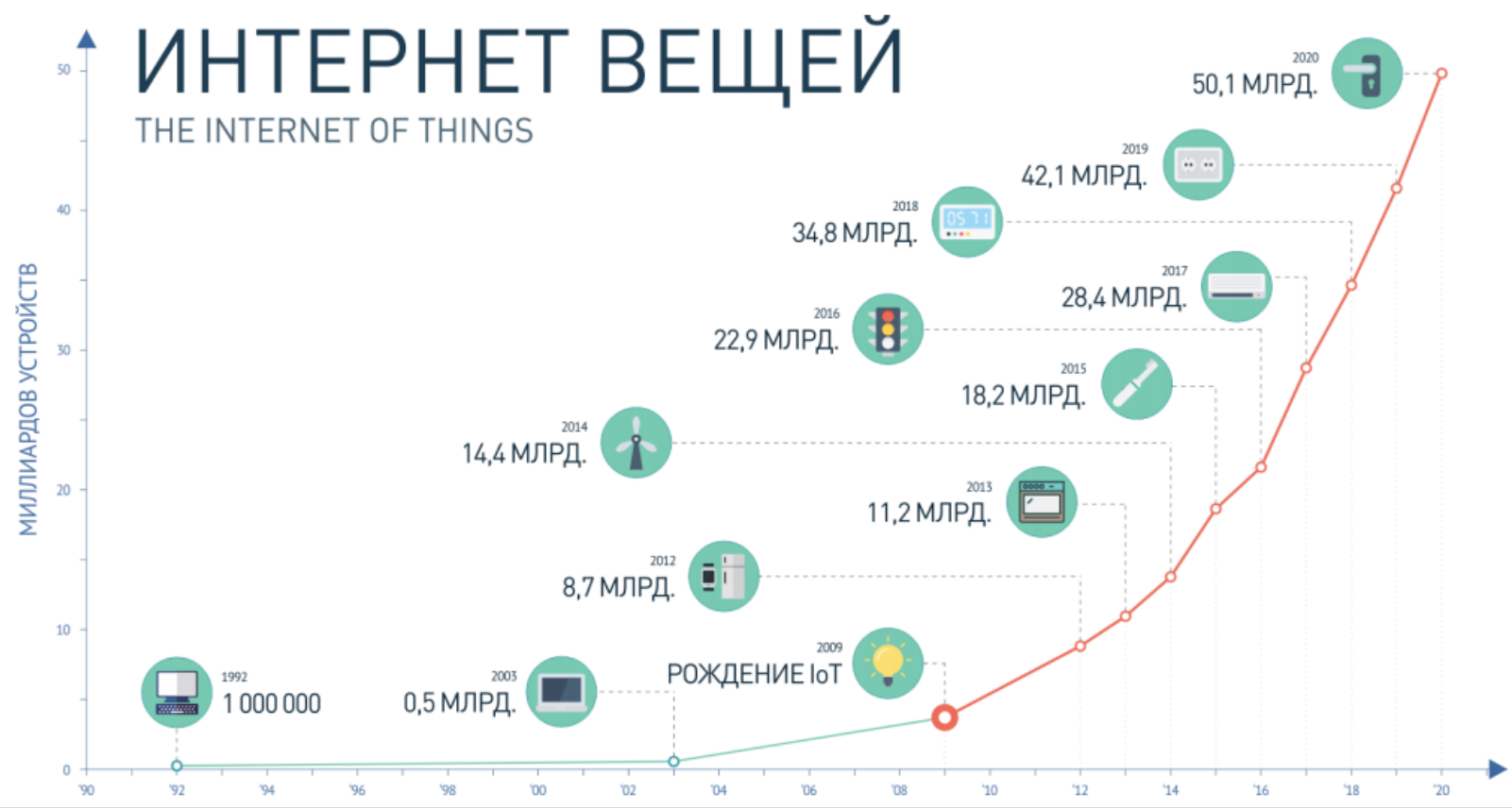
Основные локальные нормативные акты

- Инструкция администратора информационной безопасности
- Инструкция менеджера обработки персональных данных
- Положение по обработке персональных данных
- Положение об обеспечении безопасности персональных данных
- Уведомление об обработке персональных данных
- Политика о защите персональных данных
- Регламент по учёту, хранению и уничтожению носителей персональных данных
- Регламент по допуску лиц к обработке персональных данных
- Регламент по реагированию на запросы субъектов персональных данных
- Регламент по взаимодействию с органами государственной власти в области персональных данных
- Регламент по резервному копированию персональных данных
- Регламент по реагированию на инциденты информационной безопасности
- Форма Согласия на обработку персональных данных
- Технический паспорт информационных систем персональных данных
- Перечень должностей и третьих лиц, допущенных к обработке персональных данных
- Модель нарушителя безопасности персональных данных при их обработке в информационных системах персональных данных
- Приказ о назначении лиц, ответственных за обработку и защиту персональных данных

Телемедицина и Пдн

С принятием закона по телемедицине и решением вопроса о том, в каких форматах будут оказываться услуги, в 152-ФЗ,скорее всего, будут внесены поправки и дополнения, которые помогут сформировать четкие стандарты информационной безопасности.

Мир медицинских интернет вещей



К стандартным рискам и угрозам информационной безопасности, мир телемедицины приносит новые, недооценка которых может в дальнейшем привести к массовым утечкам,

Дополнительные риски в телемедицине

- Компании, которые занимаются разработкой устройств, мобильных приложений, программного обеспечения в первую очередь направлены на захват рынка для получения максимальной экономической выгоды, поэтому не всегда в должной мере уделяют внимание именно безопасности, так как это требует дополнительного тестирования и привлечение специалистов по информационной безопасности.

- Отсутствуют профильные комитеты, регламентирующие стандарты, протоколы и сервисы. Каждый производитель использует собственные удобные ему протоколы, а это крайне усложняет применение стандартных средств защиты информации, и заставляет изучать дополнительные угрозы и строить специализированные средства защиты.

- Многие устройства не предполагают возможности обновления, при этом срок эксплуатации весьма высок, то есть уязвимость, заложенная производителем будет сохраняться весь срок полезного использования.

- Некоторые устройства работают таким образом, что пациент не имеет или почти не имеет представления о внутреннем функционировании устройства, не говоря уже о его контроле.

Дополнительные риски в телемедицине

- Отсутствуют функции предупреждения об возникновении проблем с безопасностью.

- Использование бреши в безопасности одного устройства, чтобы захватить всю сеть и передавать конфиденциальную информацию о деятельности пациента - физической, интимной, религиозной.

- Устройства используются как реперные точки, для получения контроля над другими системами, а так же могут быть использованы в качестве ботнетов.

- Стандартные учетные записи от производителя, слабая аутентификация, с отсутствием возможности изменить ее.

- Использование незащищенной облачной инфраструктуры.

- Отсутствие шифрования при передаче данных, иногда передача осуществляется в текстовом формате.

- Обеспечение физической безопасности.

Необходимые меры для обеспечение безопасности mIOT

- Госрегулирование и стандартизацию протоколов, сервисов между устройствами.

- Надлежащую защиту как при передаче, так и при хранении всех собранных личных данных с возможностью ограничением доступа.

- При необходимости деидентификацию или деперсонализацию данных.

- Минимизацию сбора личной информации от пациента. Четко регламентировать объем передаваемой информации.

- Проведение просветительской и образовательной деятельности, как среди пациентов, так и среди медицинского персонала как важнейшего фактора, направленного на снижение рисков утечки информации.

- Разработка специализированных средств защиты информации с учетом медицинской специфики.

Основные средства защиты информации (СЗИ)
Антивирус

Антивирусные программы - современные антивирусные программы обеспечивают комплексную защиту программ и данных на компьютере от всех типов вредоносных программ и методов их проникновения на компьютер: Интернет, локальная сеть, электронная почта, съемные носители информации. Для защиты от вредоносных программ каждого типа в антивирусе предусмотрены отдельные компоненты. Принцип работы антивирусных программ основан на проверке файлов, загрузочных секторов дисков и оперативной памяти и поиске в них известных и новых вредоносных программ.

Антивирусное программное обеспечение

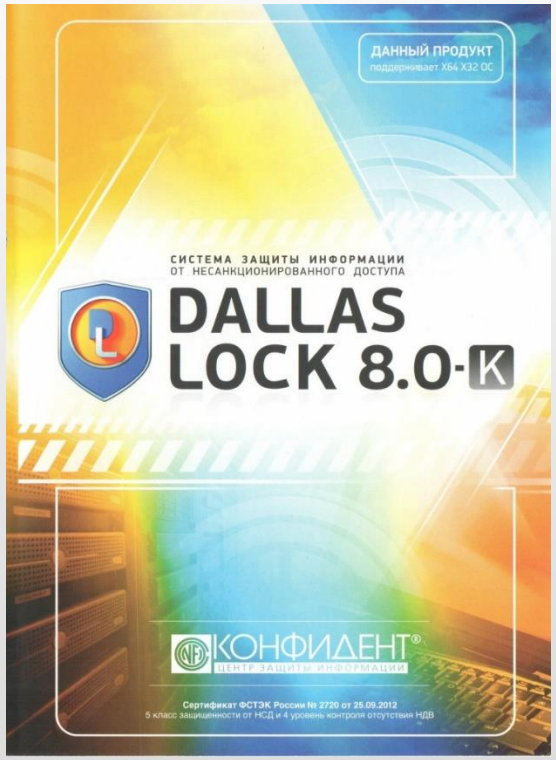
Антивирусное ПО может использовать следующие методы обнаружения вирусов и других вредоносных программ:

- сканирование;
- эвристический анализ(блокирование подозрительных действий)
- CRC-сканирование(обнаружение изменений);
- анализ сетевого трафика;
- анализ баз данных почтовых программ;
- обнаружение вирусов в системе автоматизации документооборота.
- информацию о содержании жесткого диска с елью составления

списка ПО, установленного на компьютере у пользователя;

- информацию о нажатых клавишах(клавиатурные шпионы);
- приложения, с которыми работает пользователь;
- сведения о посещении Web-сайтов и другой активности в Интернете;
- содержимое сообщений электронной почты

Основные средства защиты информации (СЗИ) Средства от Несанкционированного доступа.

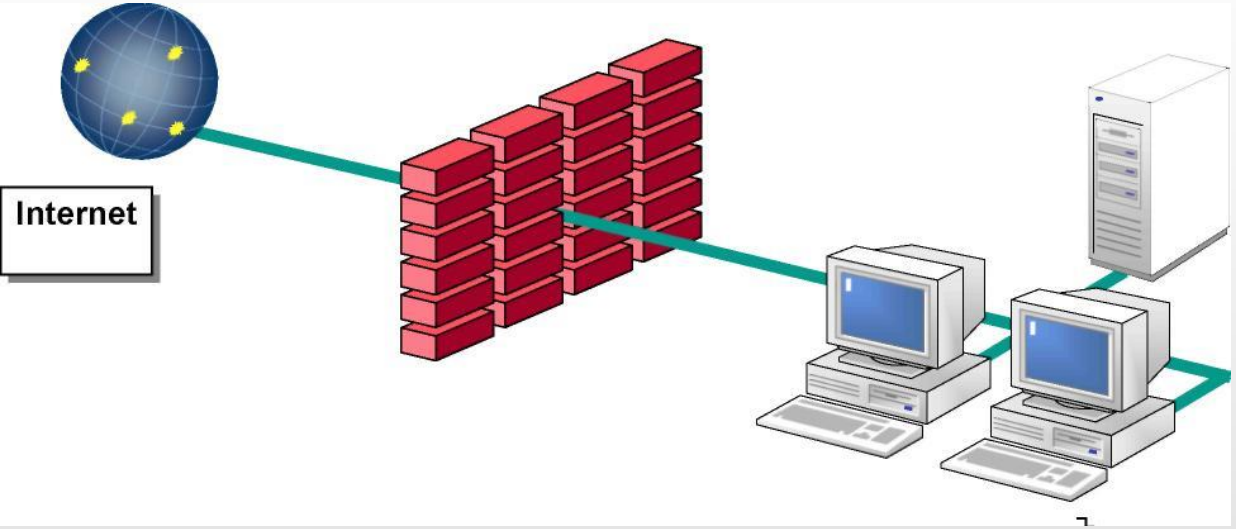


Несанкционированный доступ к информации (НСД) — это доступ к данным, который нарушает правила разграничения доступа с реализацией определенных средств которые являются средствами вычислительной техники или автоматизированными системами.

Основные средства защиты информации (СЗИ)
Средства от Несанкционированного доступа.

Управление доступом.
Протоколирование и аудит.
Шифрование.
Экранирование.
Туннелирование.
Контроль целостности.
Контроль защищенности.
Обнаружение отказов и оперативное восстановление.
Управление.

Основные средства защиты информации (СЗИ)
Межсетевые экраны

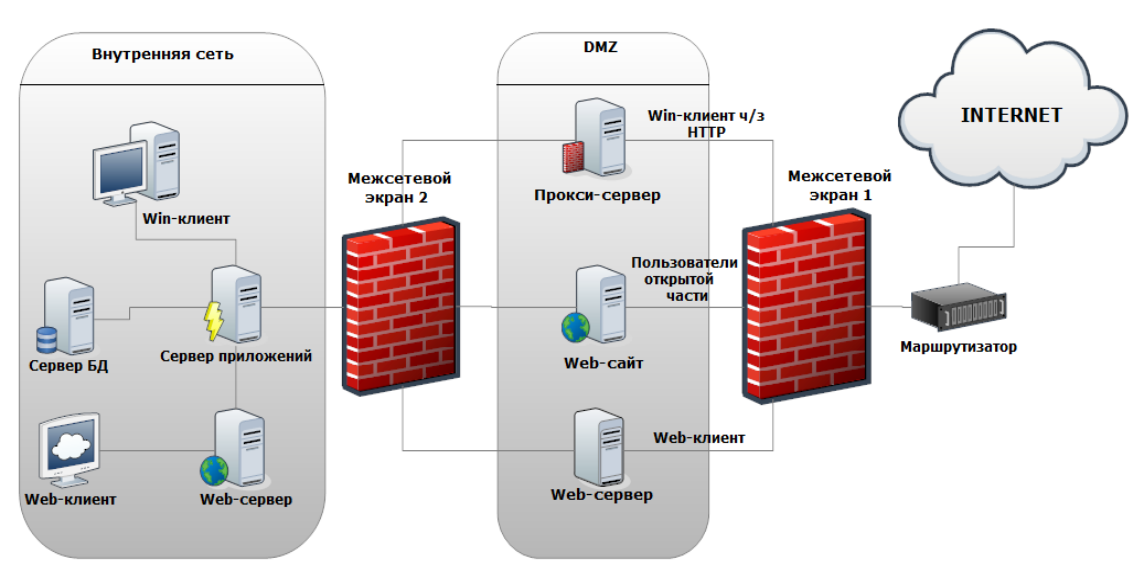


Межсетевой экран (МСЭ) — это устройство обеспечения безопасности сети, которое осуществляет мониторинг входящего и исходящего сетевого трафика и на основании установленного набора правил безопасности принимает решения, пропустить или блокироват конкретный трафик.

Межсетевые экраны используются в качестве первой линии защиты сетей уже более 25 лет. Они ставят барьер между защищенными, контролируемыми внутренними сетями, которым можно доверять, и ненадежными внешними сетями, такими как Интернет.

Межсетевой экран может быть аппаратным, программным или смешанного типа.

Основные средства защиты информации (СЗИ)
Межсетевые экраны



•Обеспечение доступа компьютеров локальной сети к сети Интернет.

•Сжатие данных: прокси-сервер загружает информацию из Интернета и передаёт информацию конечному пользователю в сжатом виде.

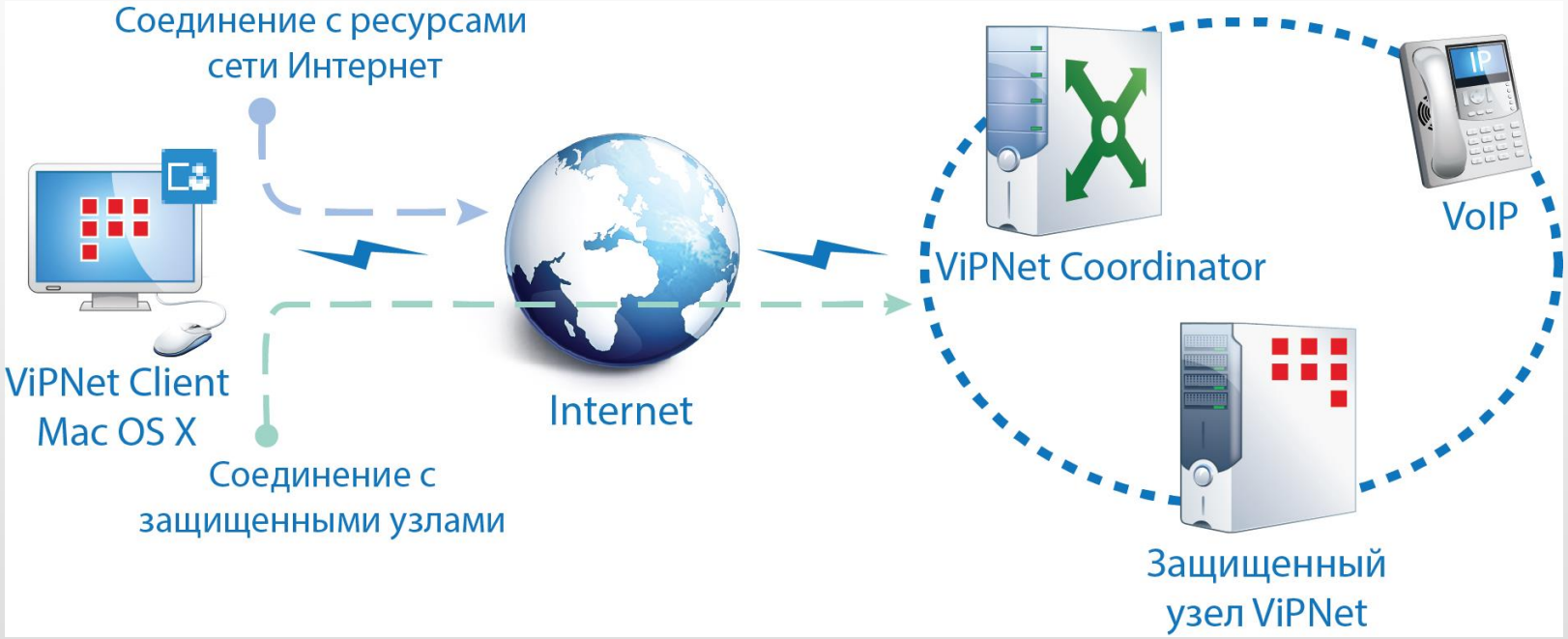
•Защита локальной сети от внешнего доступа: например, можно настроить прокси-сервер так, что локальные компьютеры будут обращаться к внешним ресурсам только через него, а внешние компьютеры не смогут обращаться к локальным вообще (они «видят» только прокси-сервер).

•Ограничение доступа из локальной сети к внешней: например, можно запрещать доступ к определённым веб-сайтам, ограничивать использование интернета каким-то локальным пользователям, устанавливать квоты на трафик или полосу пропускания, фильтровать рекламу и вирусы.

•Анонимизация доступа к различным ресурсам. Прокси-сервер может скрывать сведения об источнике запроса или пользователе. В таком случае целевой сервер видит лишь информацию о прокси-сервере.

Основные средства защиты информации (СЗИ) VPN.

ViPNet®
Virtual Private Network



ViPNet Client (Клиент) — это программный комплекс, выполняющий на рабочем месте пользователя или сервере с прикладным ПО функции VPN-клиента, персонального сетевого экрана, клиента защищенной почтовой системы, а также криптопровайдера для прикладных программ, использующих функции подписи и шифрования.

Основные средства защиты информации (СЗИ) VPN.

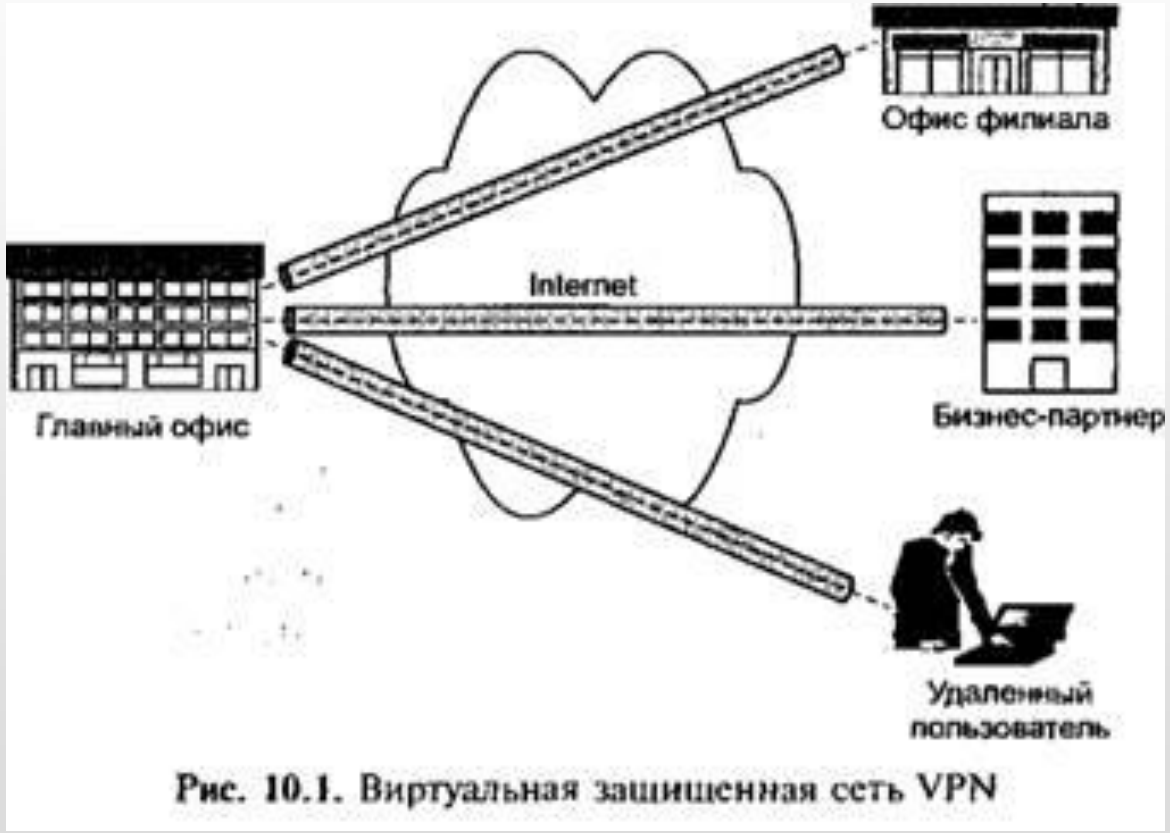


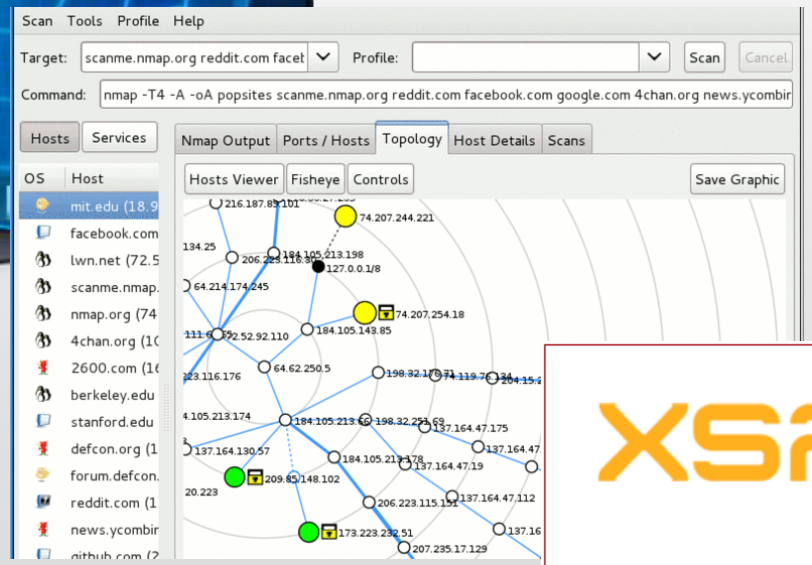
Рис. 10.1. Виртуальная защищенная сеть VPN

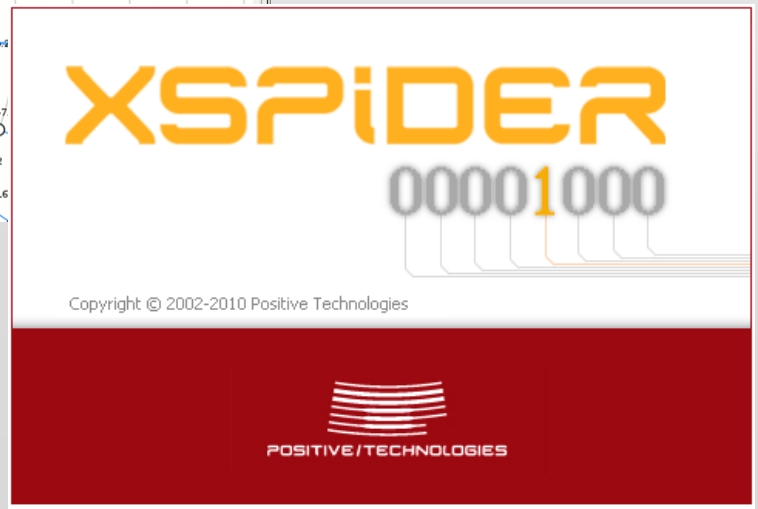
Обеспечение безопасности информационного взаимодействия локальных сетей и отдельных компьютеров через открытые сети, в частности через сеть Интернет, возможно путем эффективного решения следующих задач:

• защита подключенных к открытым каналам связи локальных сетей и отдельных компьютеров от несанкционированных действий со стороны внешней среды;

• защита информации в процессе ее передачи по открытым каналам связи.

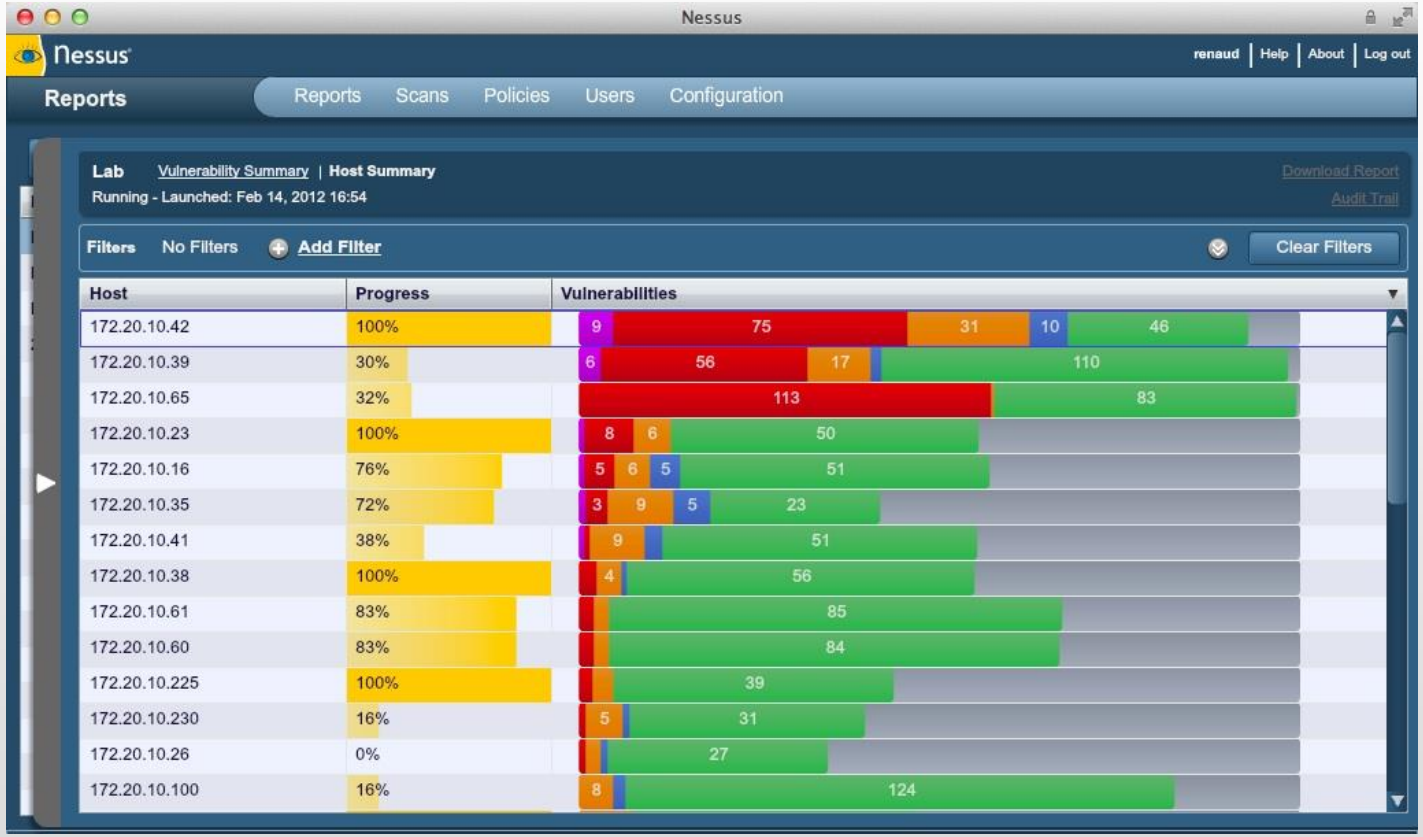
Основные средства защиты информации (СЗИ)
Сканер уязвимостей.





Сканеры уязвимостей — это программные или аппаратные средства, служащие для осуществления диагностики и мониторинга сетевых компьютеров, позволяющее сканировать сети, компьютеры и приложения на предмет обнаружения возможных проблем в системе безопасности, оценивать и устранять уязвимости.

Основные средства защиты информации (СЗИ)
Сканер уязвимостей.

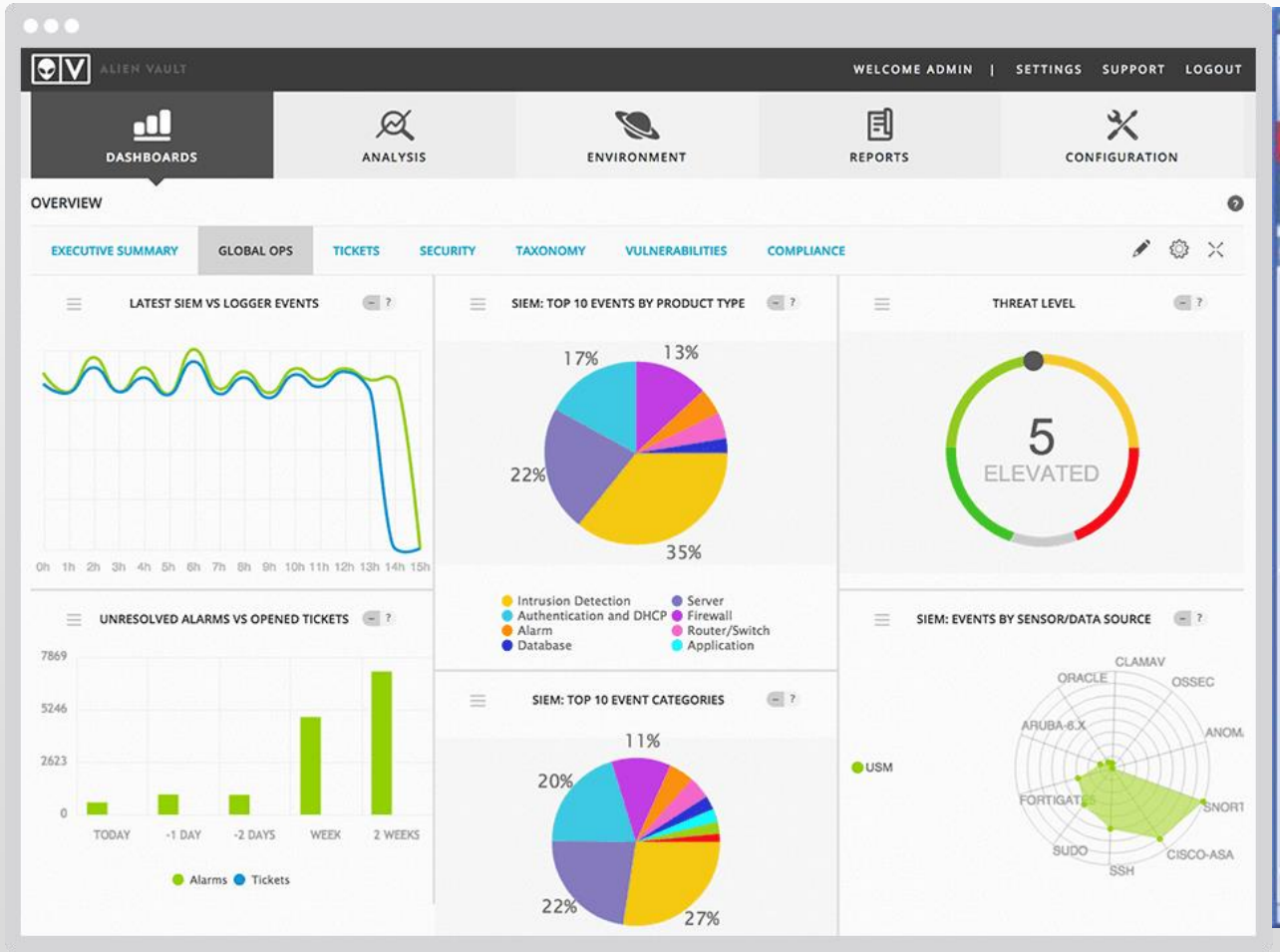


Среди сканеров уязвимостей можно выделить:

- Сканер портов
- Сканеры, исследующие топологию компьютерной сети
- Сканеры, исследующие уязвимости сетевых сервисов
- Сетевые черви
- CGI-сканеры ("дружественные" — помогают найти уязвимые скрипты)

.

Комплексные системы управления безопасностью



Комплексные системы управления безопасностью

- централизованный сбор и консолидация, хранение событий ИБ;
- агрегация событий ИБ;
- корреляция и обнаружение инцидентов ИБ в режиме реального времени;
- приоритезация инцидентов на базе матрицы критичности ресурсов;
- визуализация в различных режимах функционирования;
- эффективное расследование инцидентов и определение основных причин нарушения политики безопасности;
- ретроспективный анализ событий ИБ;
- информирование операторов и взаимодействие с исполнительными механизмами реагирования.

Сеченовский Университет
наук о жизни

Спасибо за внимание!

Рябков Илья Валерьевич
Старший преподаватель

Сеченовский Университет
наук о жизни

Практическое занятие. Основы информационной безопасности

Рябков И.В.

Основа информационной безопасности

Сеченовский Университет
наук о жизни

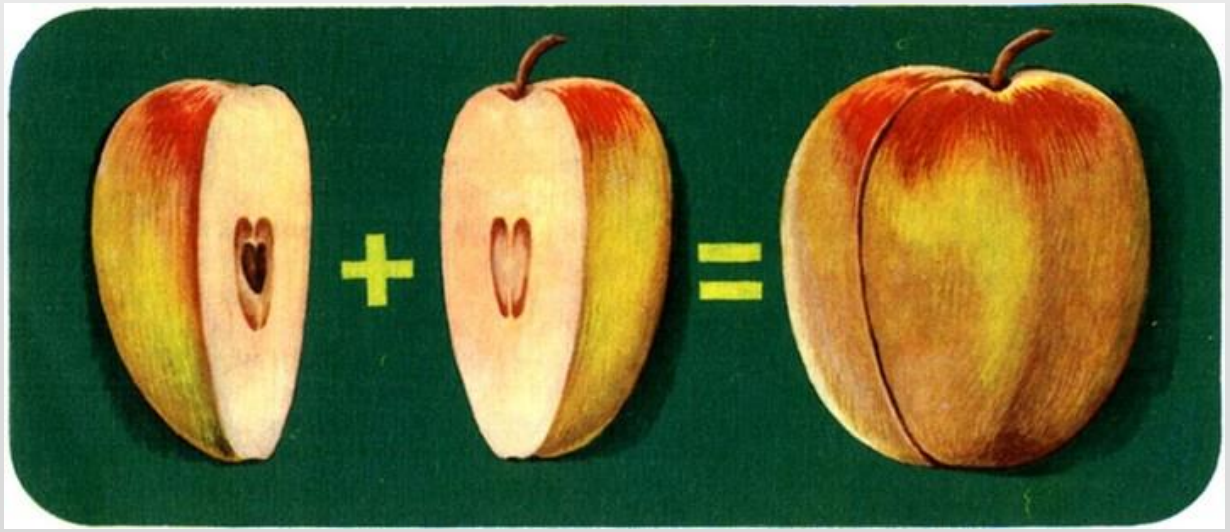
Безопасность начинается в нашей голове.

От безопасности до безумия один шаг.

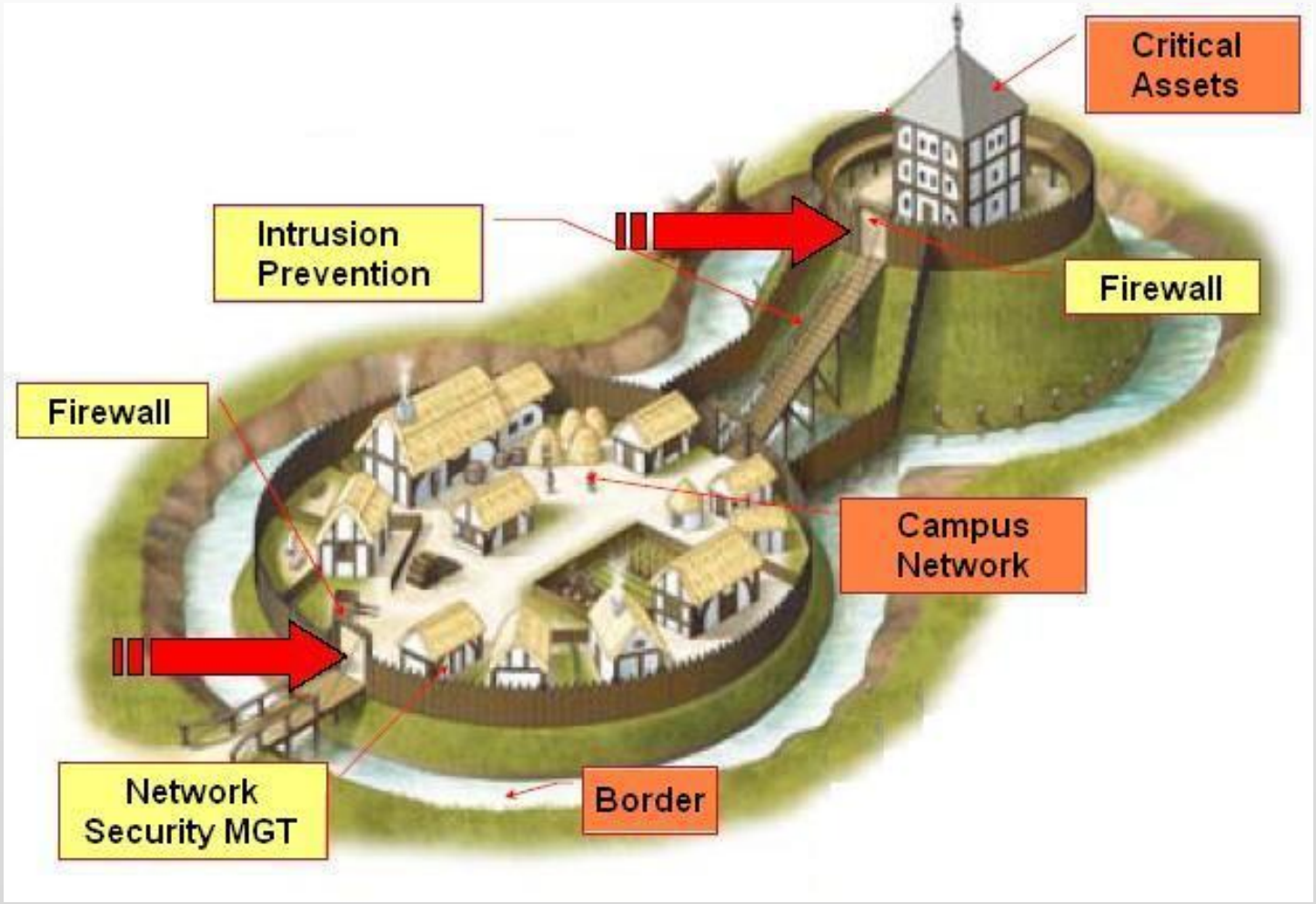
Ощущение безопасности самая опасная иллюзия

Информационная безопасность

Информационная безопасность - комплекс организационных, технических мер по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе.



Модель DEFENSE IN DEPTH
Глубокоэшелонированная защита



Основные виды информационных угроз

Угроза «информационной безопасности» – это потенциальная возможность нарушения режима

Основные принципы построения системы информационной безопасности

- Законность
- Системность
- Комплексность
- Непрерывность
- Своевременность
- Преемственность и непрерывность совершенствования
- Разумная достаточность
- Персональная ответственность
- Разделение функций
- Минимизация полномочий
- Взаимодействие и сотрудничество
- Гибкость системы защиты
- Простота применения средств защиты

Основные виды несанкционированного воздействия на информацию

- Модификация
- Уничтожение
- Искажение
- Подделка
- Блокировка доступа
- Хищение носителя

Виды нарушителей информационной безопасности

Нарушитель – лицо, предпринявшее попытку выполнения запрещенных операций по ошибке, незнанию или осознано со злым умыслом(из корыстных интересов, или без такового и использующие для этого различные возможности, методы и средства

- Внутренние (пользователи, персонал, руководители различных уровней)

- Внешние (Внешние разработчики, конкуренты, клиенты, технический персонал)

Система нормативно-правовых актов по защите информации

Сеченовский Университет
наук о жизни

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

ПП РФ от 01 ноября 2012 **№ 1119**

ПП РФ от 15 сентября 2008 **№ 687**

ПП РФ от 06 июля 2008 **№ 512**

ПП РФ от 03 ноября 1994 № 1233

ПП РФ от 4 … 2010 г. N 125

Федеральный Закон номер128-ФЗ Закон «О лицензировании отдельных видов деятельности»

Закон «О коммерческой тайне» № 98-ФЗ от 2004 года

Приказ Роскомнадзора от 5 сентября … требований и методов по обезличивани… …утверждении …нных»

Приказ ФСТЭК, ФСБ, Мининформсвязи от 13 декабря 2013 № 151/786/461

Приказ ФСТЭК РФ от 18 февраля 2013г. № 21

Приказ ФСБ РФ от 09 февраля 2005 № 66

Методические документы ФСБ

Методические документы ФСТЭК

Указ Президента РФ от 06 марта 1997 № 188 «Об утверждении перечня …ений конфиденциального …ктера»

… Президента РФ от 30 мая 2005 **… 609** «Об утверждении Положения о персональных данных государственного гражданского служащего РФ и ведении его личного дела»

Указ Президента РФ от 17 марта 2008 **№ 351** «О мерах по обеспечению информационной безопасности РФ при использовании информационно-телекоммуникационных сетей международного информационного обмена»

Трудовой кодекс РФ «Защита персональных данных работника»

ФЗ закон от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Закон «О государственной тайне» от 21 июля 1993 годаN 5486-1

Государственные стандарты

- ГОСТ Р 51275-2006. «Объект информации. Факторы, воздействующие на информацию. Общие положения»;
- ГОСТ 34.003-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения»;
- ГОСТ 34.201-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании информационных систем»;
- ГОСТ 34.601-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы.. Стадии создания»;
- ГОСТ 34.602-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;
- ГОСТ Р 51624-2000. «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования»;
- ГОСТ Р 50922-2006. «Защита информации. Основные термины и определения»;
- ГОСТ Р 53114-2008. «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения»;
- ГОСТ Р ИСО/МЭК 15408-1-2008. «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель»;
- ГОСТ Р 51583-2014. «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

Контролирующие органы в области защиты персональных данных

Роскомнадзор

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций

Орган по защите прав субъектов Пдн

ФСТЭК

Федеральная служба по техническому и экспортному контролю

Федеральный орган, уполномоченный в области противодействия техническим разведкам и технической защиты информации

ФСБ

Федеральная служба безопасности

Федеральный орган, уполномоченный в области обеспечения безопасности

Роструд

Федеральная служба по труду и занятости

Федеральный орган, по контролю и надзору за соблюдением трудового законодательства и иных нормативных правовых актов, содержащих нормы трудового права

Информационная безопасность. Виды ответственности.

Сеченовский Университет
наук о жизни

Гражданская ответственность

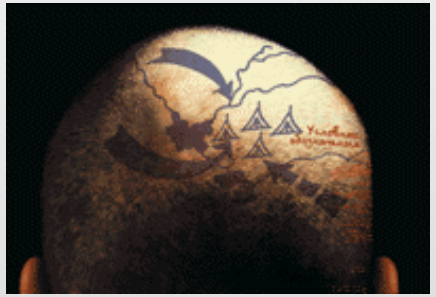
Дисциплинарная ответственность

Административная ответственность

Уголовная ответственность

Три способа защиты информации

Силовые методы: охрана документа (носителя информации) физическими лицами, его передача специальным курьером

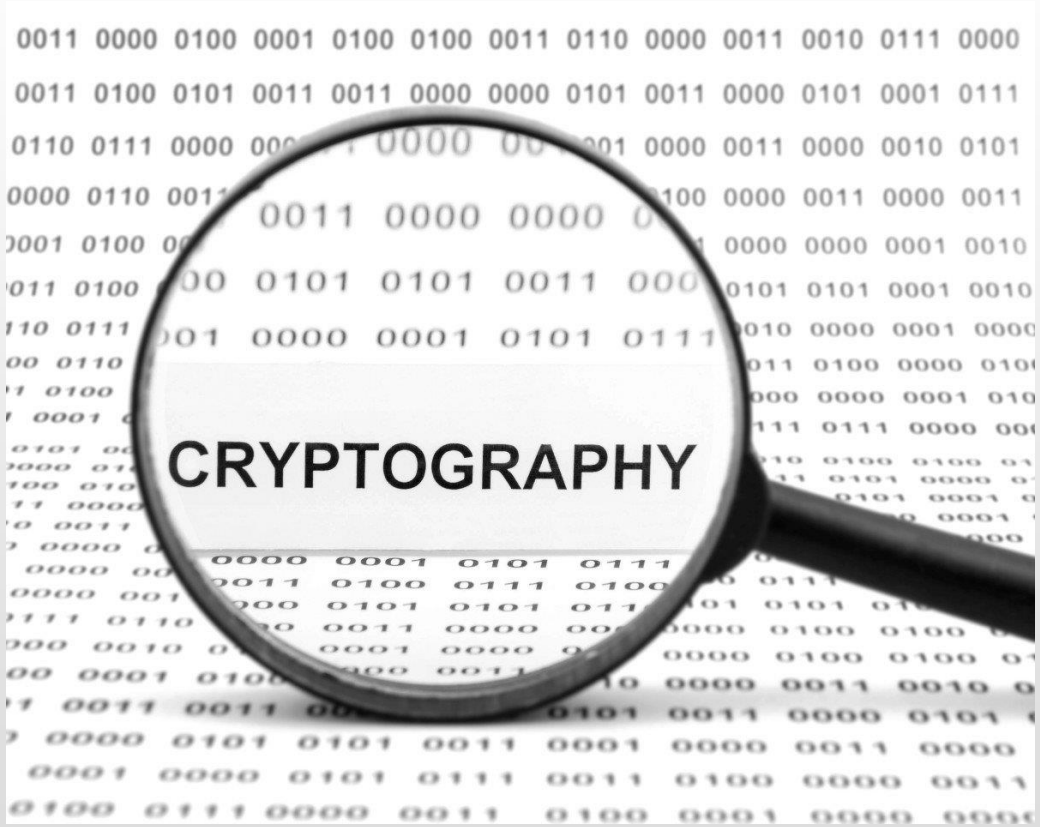


Сокрытии самого факта наличия секретной информации. В этом случае, в частности, использовались так называемые «симпатические чернила».

Криптографическая защита информации, путем преобразование текста в хаотический набор знаков.

Криптография. История возникновения

Сеченовский Университет
наук о жизни



Наука о тайной передачи информации, недоступной или непонятной для посторонних лиц, произошло и стало развиваться в тот момент, когда человечество осознало необходимость обеспечения защиты информации.

Криптография – одна из старейших наук, ее история насчитывает несколько тысяч лет, развиваясь вместе с человеком, она претерпела огромное количество изменений, постоянно совершенствуясь и дополняясь. Криптографическая защита информации является одной из основных подсистем любой системы защиты информации(СЗИ).

Во все исторические времена существенное внимание уделялось проблеме информационной безопасности, обеспечению защиты конфиденциальной информации от ознакомления с ней конкурирующих групп.

Криптография. Наука и жизнь

Сеченовский Университет
наук о жизни

Криптография– это раздел прикладной математики, изучающий модели, методы, алгоритмы, программные и аппаратные средства преобразования информации (шифрования) в целях сокрытия ее содержания, предотвращения видоизменения или несанкционированного использования.

Криптография тесно связанна с различными областями технических дисциплин таких как: математика (алгебра, теория вероятности, теория сложности, теория чисел, вычислительная математика и т.д.), теория связи, теория кодирования.

Криптография. Основные понятия и определения

Сеченовский Университет
наук о жизни

Криптографическая защита – защита данных при помощи криптографического преобразования данных.

Криптосистема– это система, реализованная программно, аппаратно или программно – аппаратно и осуществляющая криптографическое преобразование информации.

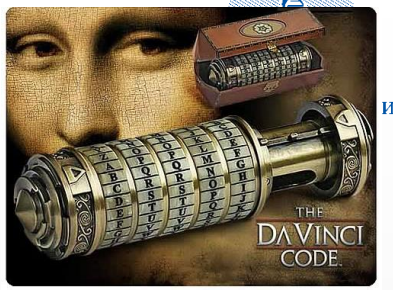
Криптоанализ– это раздел прикладной математики, изучающий модели, методы, алгоритмы, программные и аппаратные средства анализа криптосистемы или ее входных и выходных сигналов с целью извлечения конфиденциальных параметров, включая открытый текст.

Криптология– наука, объединяющая криптографию и криптоанализ.

Открытый текст (сообщение) – это текст, подлежащий криптографической защите.

Ключ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразования. Все криптосистемы должны иметь средства управления ключами. Создание, передача и хранение ключей называется управление ключами.

Криптография. Шифрование и дешифрование

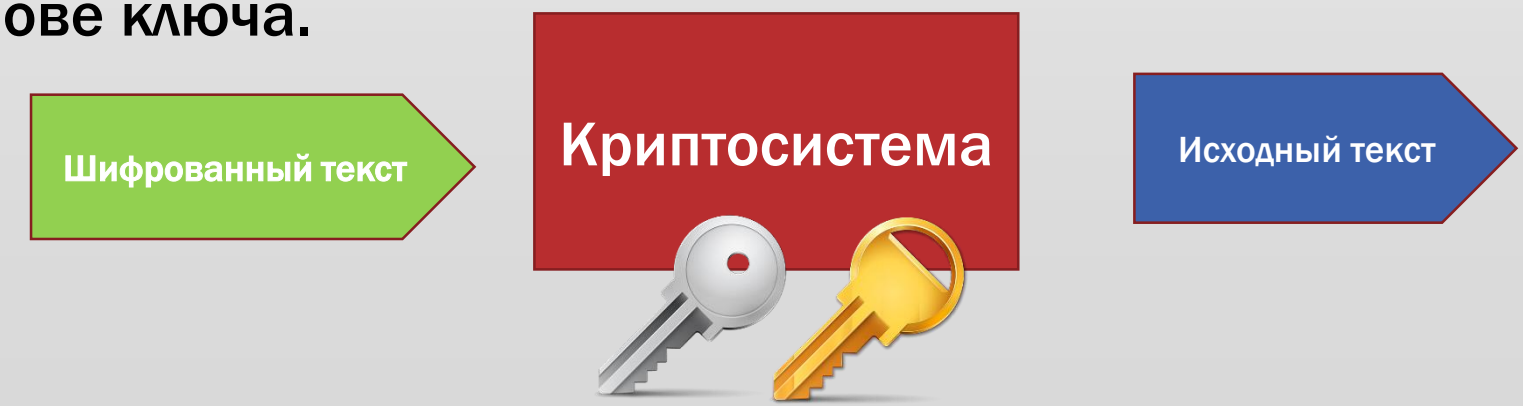


ИТЕТ

Шифрование – это преобразование данных в вид, недоступный для чтения без соответствующей информации (ключа шифрования). Шифрование обеспечивает криптографическую защиту данных от несанкционированного доступа.

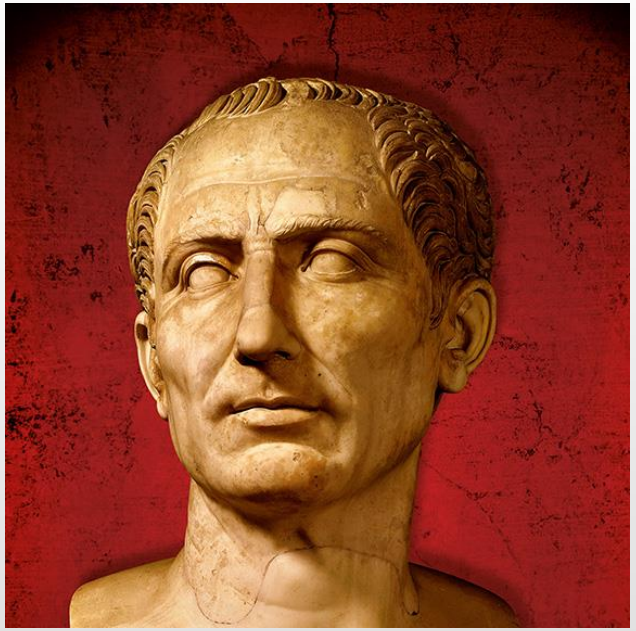
Ключ- информация необходимая для шифрования и дешифрования

Дешифрование – это обратный шифрованию процесс, на основе ключа.



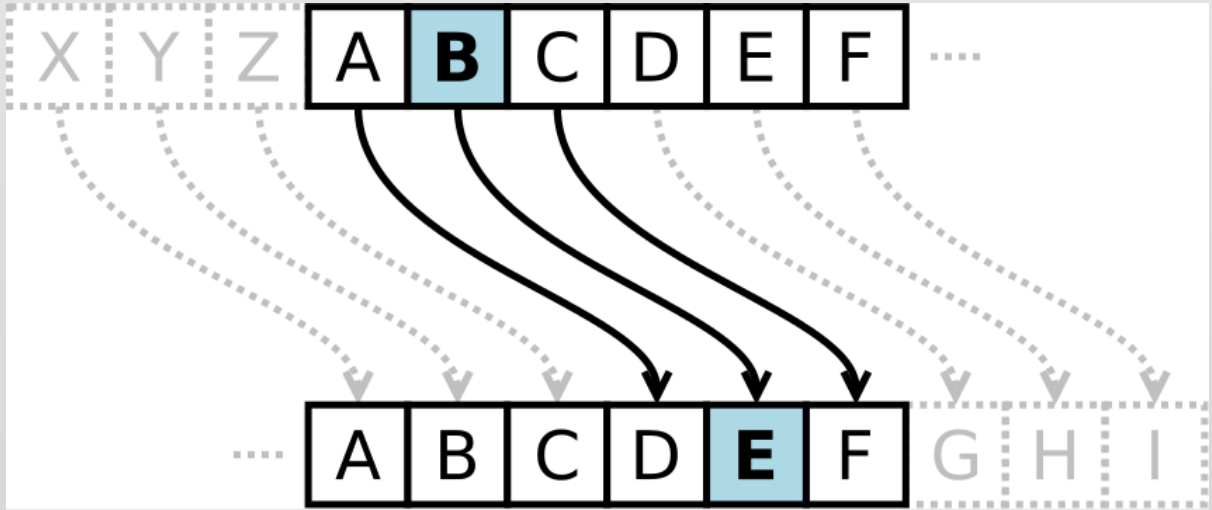
Наиболее известные шифры. Шифр Гая Юлия Цезаря

Сеченовский Университет
наук о жизни



Шифр Цезаря, также известный как **шифр сдвига**, **код Цезаря** или **сдвиг Цезаря** — один из самых простых и наиболее широко известных методов шифрования.
Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.

Древнеримский государственный и политический деятель, полководец, писатель. Консул 59, 48, 46, 45 и 44 годов до н. э., диктатор 49, 48—47 и 46—44 годов до н. э., великий понтифик с 63 года до н. э.



Наиболее известные шифры. Шифр перестановки

Сеченовский Университет
наук о жизни

НИМАРЕЛ -	МИНЕРАЛ,
ЛЕТОФЕН -	ТЕЛЕФОН,
НИЛКЙЕА -	ЛИНЕЙКА,
НОМОТИР -	МОНИТОР,
РАКДНАША -	КАРАНДАШ

Шифр перестановки — это метод симметричного шифрования, в котором элементы исходного открытого текста меняют местами. Элементами текста могут быть отдельные символы (самый распространённый случай), пары букв, тройки букв, комбинирование этих случаев и так далее. Типичными примерами перестановки являются анаграммы.

В классической криптографии шифры перестановки можно разделить на два класса:

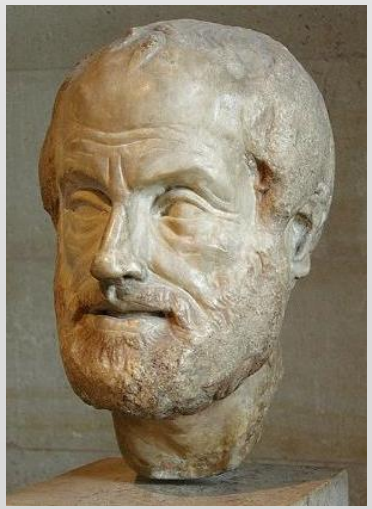
•Шифры одинарной (простой)

Наиболее известные шифры. Шифр перестановки «сцитала»

Скитала (или ***сцитала*** — от греческого *σκυτάλη*, жезл) — инструмент, используемый для осуществления перестановочного шифрования, в криптографии известный также как *шифр Древней Спарты*. Представляет собой цилиндр и узкую полоску пергамента, на которой писалось сообщение, обматывавшуюся вокруг него по спирали. Античные греки и спартанцы, предположительно, использовали этот шифр для обмена сообщениями во время военных кампаний.

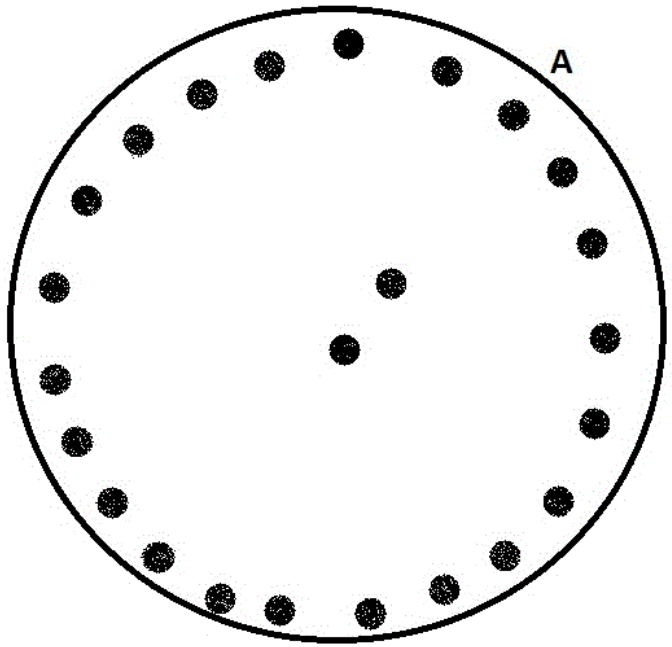
Сцитала (др. Спарта, V-VI вв. до н.э.)

Для шифрования сообщения использовались пергаментная лента и палочка цилиндрической формы с фиксированными длиной и диаметром]. Пергаментная лента наматывалась на палочку так, чтобы не было ни просветов, ни нахлёстов. Написание сообщения производилось по намотанной пергаментной ленте по длинной стороне цилиндра. После того, как достигался конец намотанной ленты, палочка поворачивалась на часть оборота и написание сообщения продолжалось. После разматывания ленты на ней оказывалось зашифрованное сообщение. Расшифрование выполнялась с использованием палочки таких же типоразмеров.



Изобретение дешифровального устройства – «антисцитала» – приписывается Аристотелю. Он предложил использовать конусообразные «копьё», на которое наматывался перехваченный ремень, этот ремень передвигался по оси до того положения, пока не появлялся осмысленный текст.

Наиболее известные шифры. Диск Энея



Диск Энея — криптографический инструмент для защиты информации, придуманный Энеем Тактиком в IV веке до н. э. Устройство представляло собой диск диаметром 13—15 см и толщиной 1—2 см с проделанными в нём отверстиями, количество которых равнялось числу букв в алфавите. Каждому отверстию ставилась в соответствие конкретная буква. В центре диска находилась катушка с намотанной на неё ниткой. При зашифровывании нитка «вытягивалась» с катушки и последовательно протягивалась через отверстия, в соответствии с буквами шифруемого текста.

Диск и являлся посланием. Получатель послания последовательно вытягивал нитку из отверстий, что позволяло ему получать передаваемое сообщение, но в обратном порядке следования букв. При перехвате диска недоброжелатель имел возможность прочитать сообщение тем же образом, что и получатель. Но Эней предусмотрел возможность легкого уничтожения передаваемого сообщения при угрозе захвата диска. Для этого было достаточно выдернуть «катушку» с закрепленным на ней концом нити до полного выхода всей нити из всех отверстий диска.

Код Да Винчи. Реальность и миф.

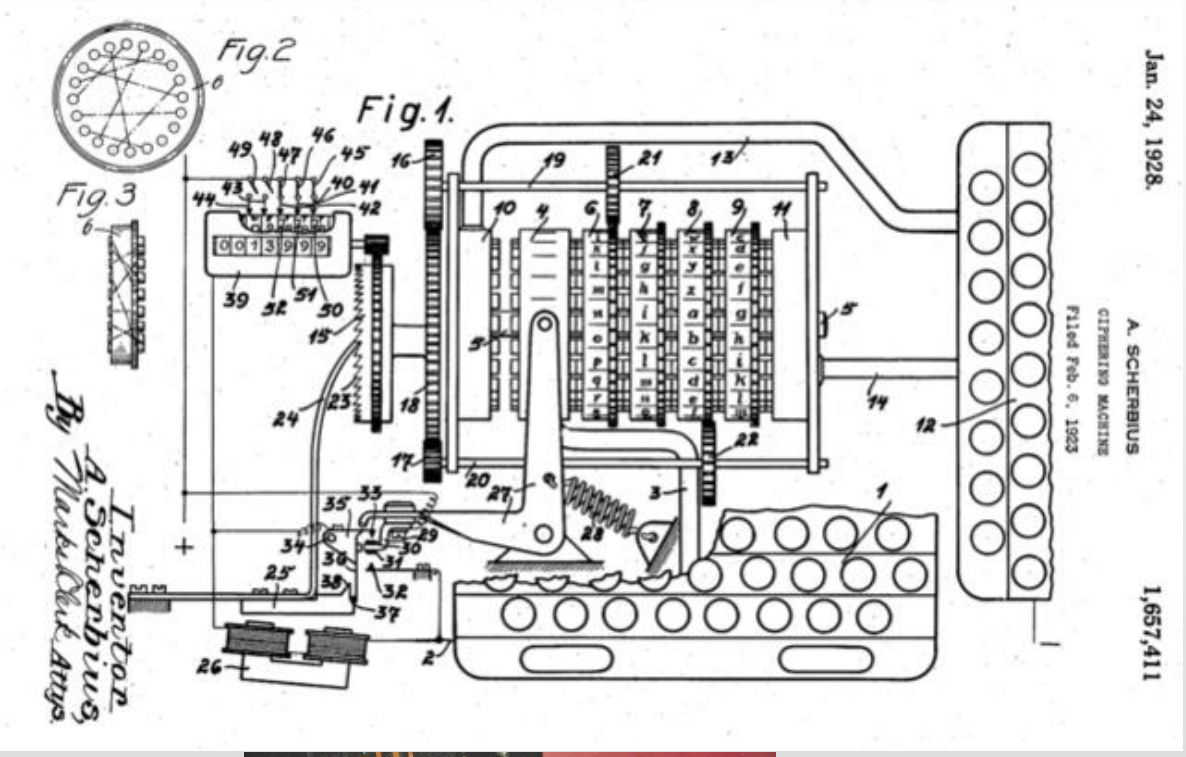
Сеченовский Университет
наук о жизни

Одной из идей книги «Код Да Винчи «является то, Леонардо да Винчи изобрел **«Криптех»,** шифровальное устройство, которое он часто использовал для зашифровки своих текстов. Однако, по Брауну он не только не смог утаить его, но практически оно не работало.

Устройство представляло собой цилиндр с набором ключей для дешифрирования (шифрования), в котором имелся сосуд с уксусом. В случае опасности папирус с ключами можно уничтожить, разбив сосуд с уксусом.
После чего папирус превращается в пульпу

В реальности, уксус не оказывает никакого эффекта на папирус.

Шифровальная машина. Энигма - 100-лет.



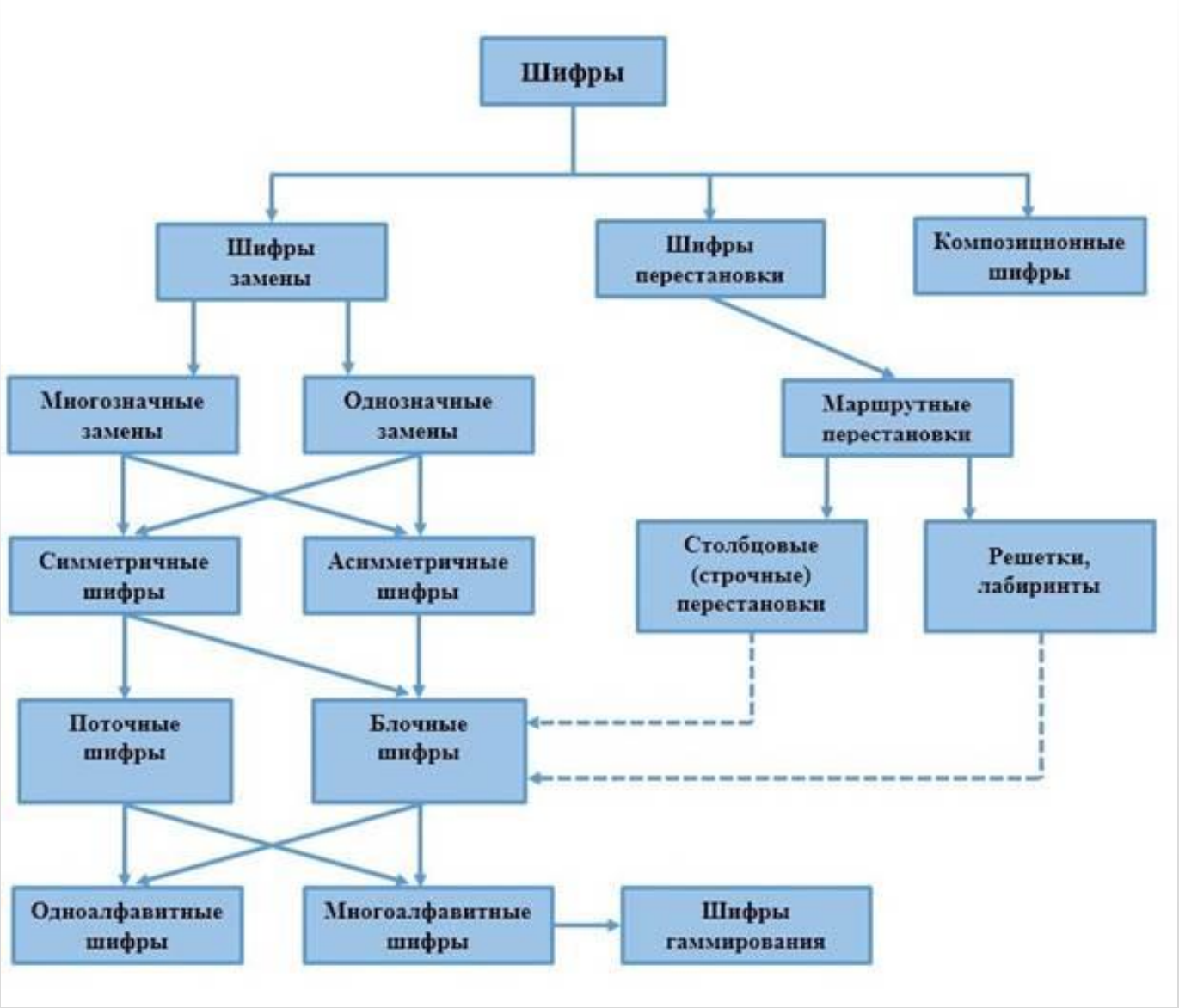
«**Эни́гма**» (от др.-греч. αἴνιγμα — загадка) — переносная шифровальная машина, использовавшаяся для шифрования и дешифрования секретных сообщений. Более точно, «Энигма» — целое семейство электромеханических роторных машин, применявшихся с 20-х годов XX века.

Впервые шифр «Энигмы» удалось расшифровать в польском Бюро шифров в декабре 1932 года. Трое сотрудников разведки, Мариан Реевский, Ежи Рожицкий и Генрих Зыгальский, с помощью данных французской разведки, математической теории и методов обратной разработки смогли разработать специальное устройство для расшифровки закодированных сообщений, которое назвали криптологической бомбой.

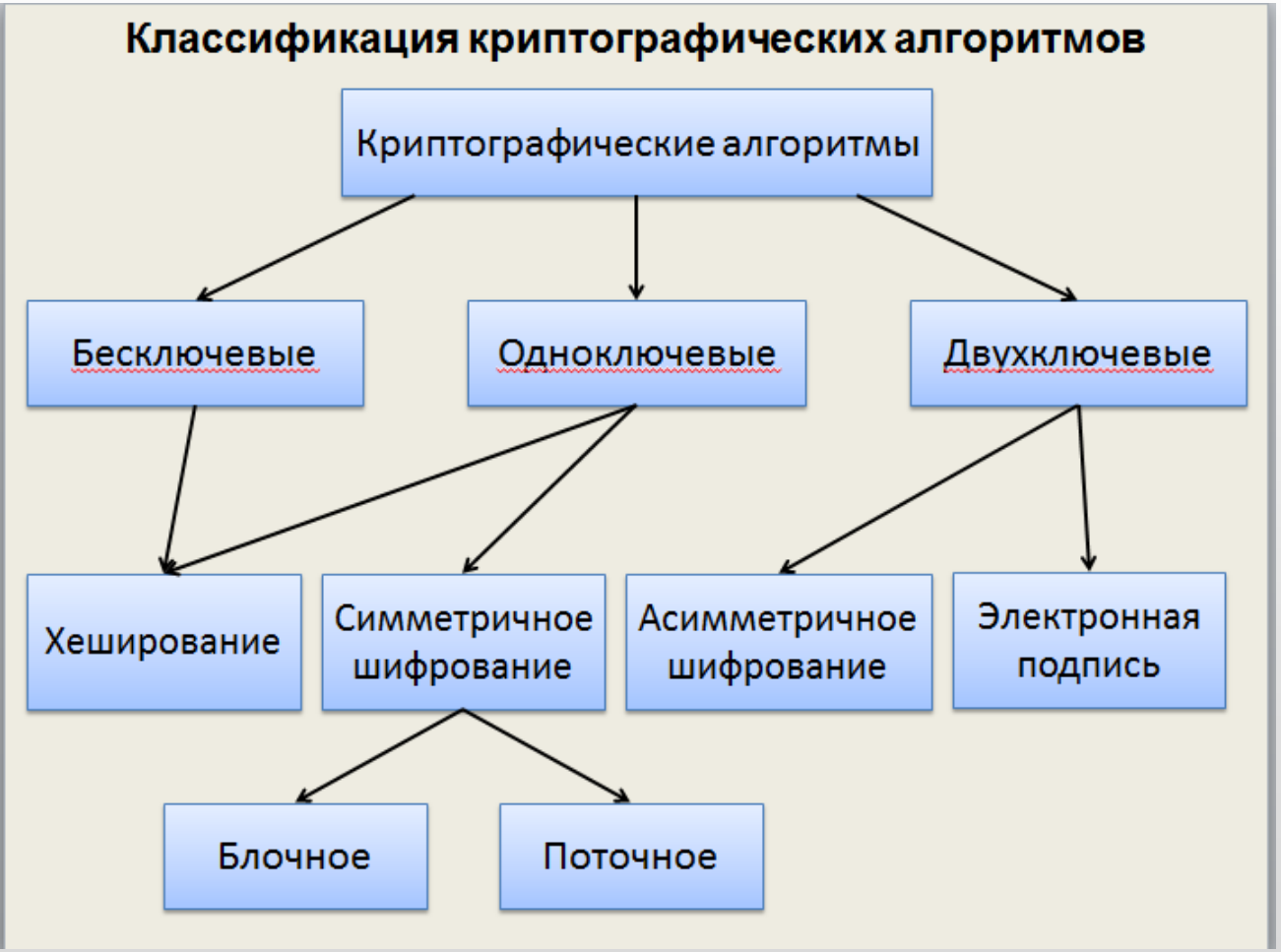
Шифровальная машина. Фиалка

Фиалка (М-125) — шифровальная машина, разработанная в СССР вскоре после Второй мировой войны. Использовалась странами Варшавского договора до 1990-х годов. Большая часть машин после распада СССР была разобрана или уничтожена. Несколько экземпляров хранятся в частных коллекциях и музеях. Работающая модель представлена в Музее компьютерной истории(Computer History Museum) в США и Блетчли-Парке (Bletchley Park) в Великобритании. В истории криптографии мало что известно о Фиалке, до 2005 года вся информация об устройстве держалась в секрете. Правильное определение "Фиалки" — кодировочная машина, поскольку она обладала более слабой криптостойкостью, чем шифровальные машины.

Классификация шифров



Классификация криптографических алгоритмов



Симметричное шифрование

Симметричные алгоритмы шифрования(или криптография с секретными ключами) основаны на том что отправитель и получатель ин-формации используют один и тот же ключ. Этот ключ должен храниться в тайне и передаваться способом, исключающим его перехват.

Обмен информацией осуществляется в 3 этапа:

1. отправитель передает получателю ключ(в случае сети с несколькими
абонентами у каждой пары абонентов должен быть свой ключ, отлич-ный от ключей других пар);
2. отправитель, используя ключ, зашифровывает сообщение, которое
пересылается получателю;
3. получатель получает сообщение и расшифровывает его.

Если для каждого дня и для каждого сеанса связи будет использо-ваться уникальный ключ, это повысит защищенность системы.

Ассиметричное шифрование

Асимметричные алгоритмы шифрования — это алогритмы, в которых для шифрования и расшифрования используются разные, но математически связанные между собой ключи. Такие связанные ключи называются криптопарой. Один из них является закрытым (private), второй является открытым (public). При этом, информация, зашифрованная на открытом ключе, может быть расшифрована только с помощью закрытого ключа, и наоборот, то что зашифрованно закрытым, можно расшифровать только с помощью открытого ключа.

Закрытый ключ Вы храните в надёжном месте, и никто, кроме Вас его не знает, а копию открытого ключа Вы раздаёте всем желающим. Таким образом, если кто-то захочет обменяться с Вами зашифрованными сообщениями, то он зашифровывает сообщение на Вашем открытом ключе, который доступен всем желающим, а расшифровать это сообщение можно будет только с помощью Вашего закрытого ключа

Хеширование

Методика хеширования использует алгоритм, известный как хэш-функция для генерации специальной строки из приведенных данных, известных как хэш. Этот хэш имеет следующие свойства: одни и те же данные всегда производит тот же самый хэш. невозможно, генерировать исходные данные из хэша в одиночку. Нецелесообразно пробовать разные комбинации входных данных, чтобы попытаться генерировать тот же самый хэш. Таким образом, основное различие между хэшированием и двумя другими формами шифрования данных заключается в том, что, как только данные зашифрованы (хешированы), они не могут быть получены обратно в первозданном виде (расшифрованы).

Этот факт гарантирует, что даже если хакер получает на руки хэш, это будет бесполезно для него, так как он не сможет расшифровать содержимое сообщения. Message Digest 5 (MD5) и Secure Hashing Algorithm (SHA) являются двумя широко используемыми алгоритмами хеширования.

Электронно-цифровая подпись

Электронная подпись (ЭП) – это особый реквизит документа, который позволяет установить отсутствие искажения информации в электронном документе с момента формирования ЭП и подтвердить принадлежность ЭП владельцу. Значение реквизита получается в результате криптографического преобразования информации.

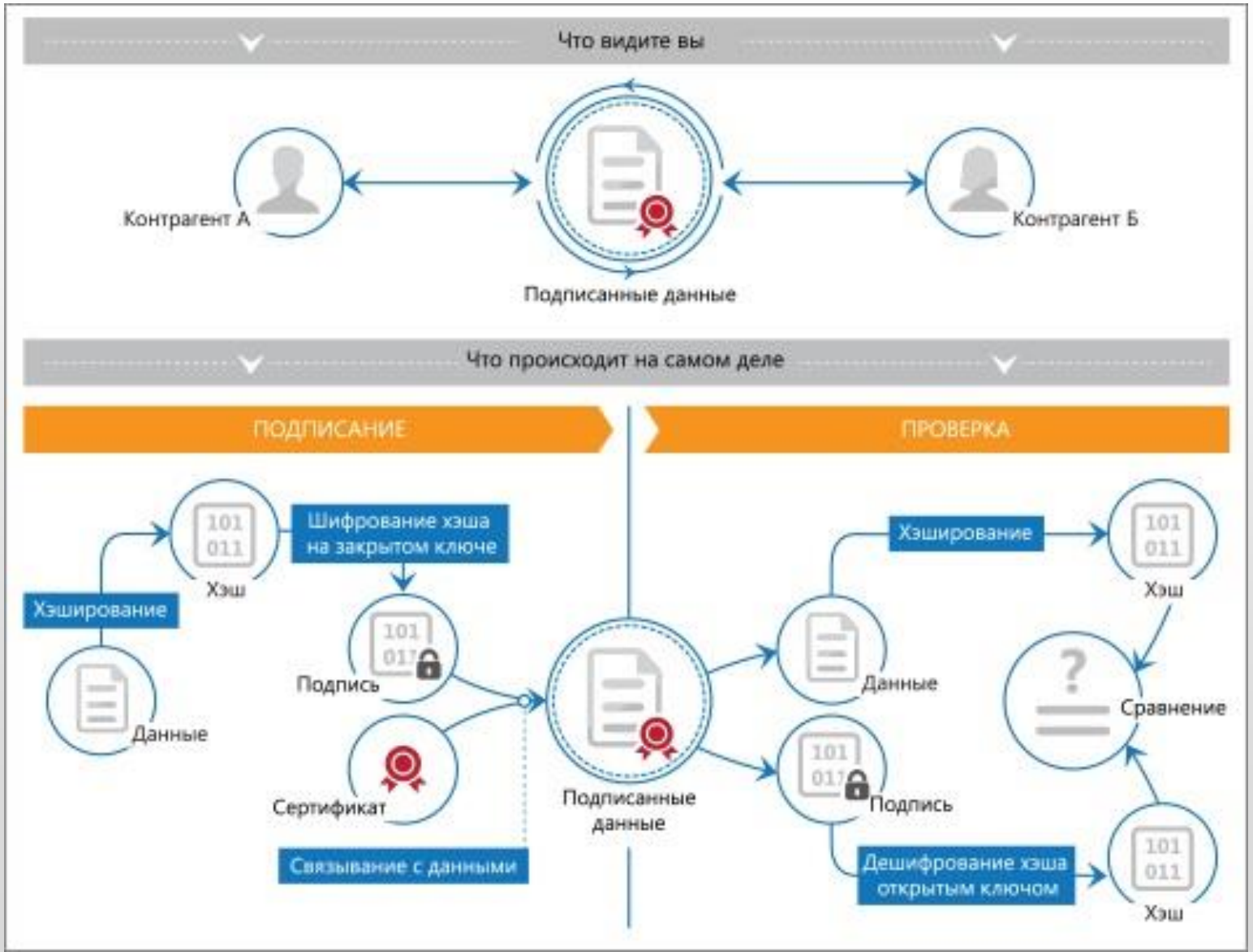
Сертификат электронной подписи – документ, который подтверждает принадлежность открытого ключа (ключа проверки) ЭП владельцу сертификата.

Владелец сертификата ЭП – физическое лицо, на чье имя выдан сертификат ЭП в удостоверяющем центре. У каждого владельца сертификата на руках два ключа ЭП: закрытый и открытый.

Закрытый ключ электронной подписи **(ключ ЭП)** позволяет генерировать электронную подпись и подписывать электронный документ. Владелец сертификат обязан в тайне хранить свой закрытый ключ.

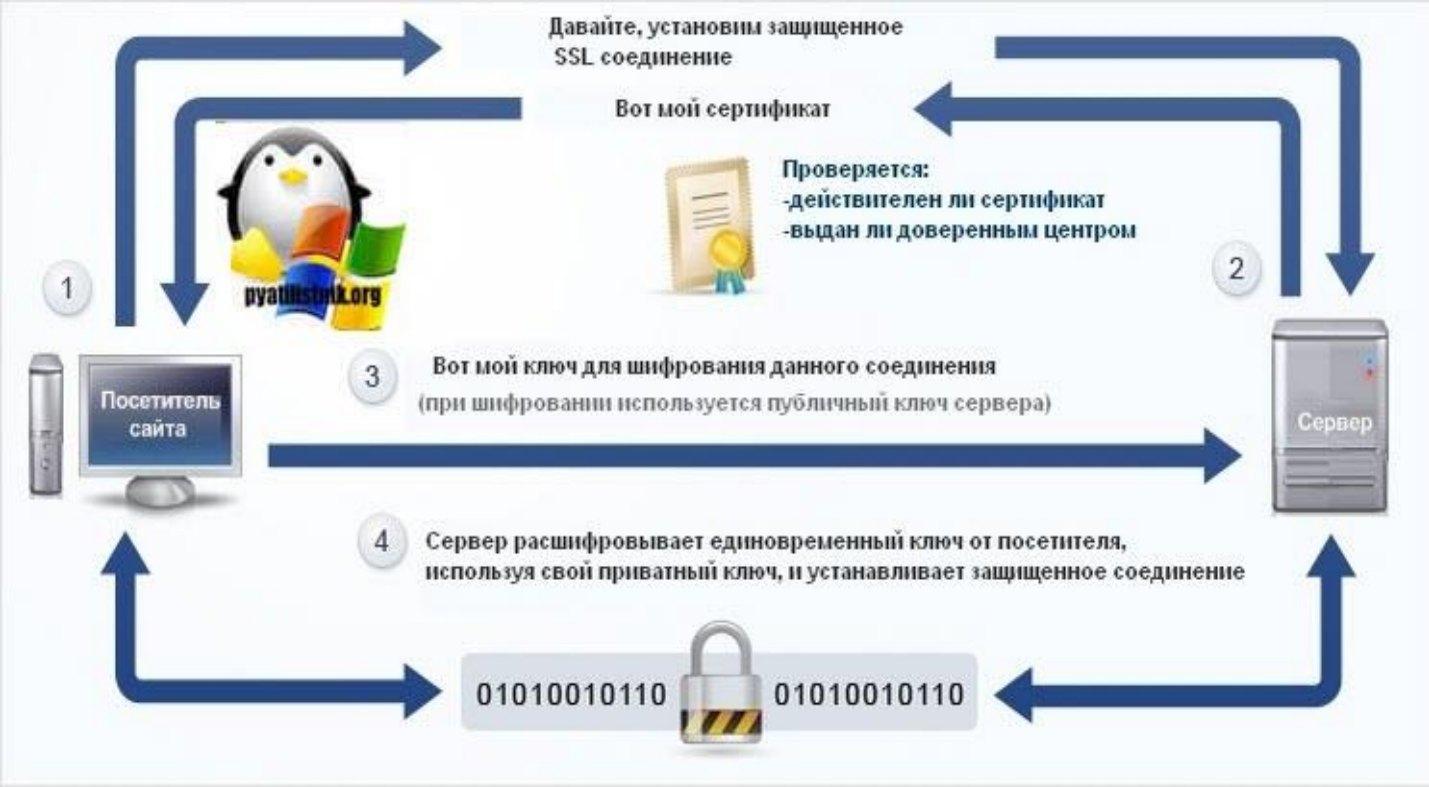
Открытый ключ электронной подписи **(ключ проверки ЭП**) однозначно связан с закрытым ключом ЭП и предназначен для проверки подлинности ЭП.

Электронно-цифровая подпись



Сертификаты SSL / TLS

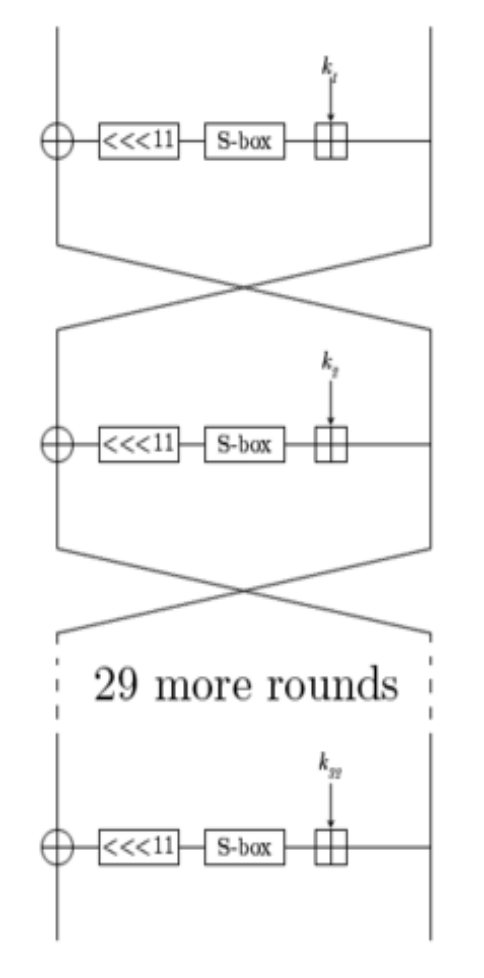
Сертификат - это двоичная структура, содержащая информацию о владельце открытого ключа.



SSL (англ. *Secure Sockets Layer* — уровень защищённых сокетов) — криптографический протокол, который подразумевает более безопасную связь. Он использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений. Протокол широко использовался для обмена мгновенными сообщениями и передачи голоса через IP

ГОСТ 28147-89 (Магма)

Российский стандарт симметричного блочного шифрования, принятый в 1989 году. **Полное название — «ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования». Является примером DES подобных криптосистем. Создатель КГБ- 8е управление**



ГОСТ 28147-89 — блочный шифр с 256-битным ключом и 32 циклами (называемыми раундами) преобразования, оперирующий 64-битными блоками. Основа алгоритма шифра — сеть Фейстеля. Выделяют четыре режима работы ГОСТ 28147-89:

Достоинства стандарта

- бесперспективность атаки полным перебором
- **эффективность реализации и, соответственно, высокое быстродействие на современных компьютерах;**
- **наличие защиты от навязывания ложных данных**

Основные проблемы стандарта связаны с неполнотой стандарта в части генерации ключей и таблиц замен. Считается, что у стандарта существуют «слабые» ключи и таблицы замен, но в стандарте не описываются критерии выбора и отсева «слабых».

ЭЦП. Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ

Настоящий Федеральный закон регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами.

электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию

Три вида ЭЦП

•**Простой электронной подписью** является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

•**Усиленной неквалифицированной электронной подписью** является электронная подпись, которая:
1.получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
2.позволяет определить лицо, подписавшее электронный документ;
3.позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
4.создается с использованием средств электронной подписи.

•**Усиленной квалифицированной электронной подписью** является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:
1.ключ проверки электронной подписи указан в квалифицированном сертификате;
2.для создания и проверки электронной подписи используются средства электронно подписи, получившие подтверждение соответствия требованиям,

Аутентификация и идентификация. Основные понятия

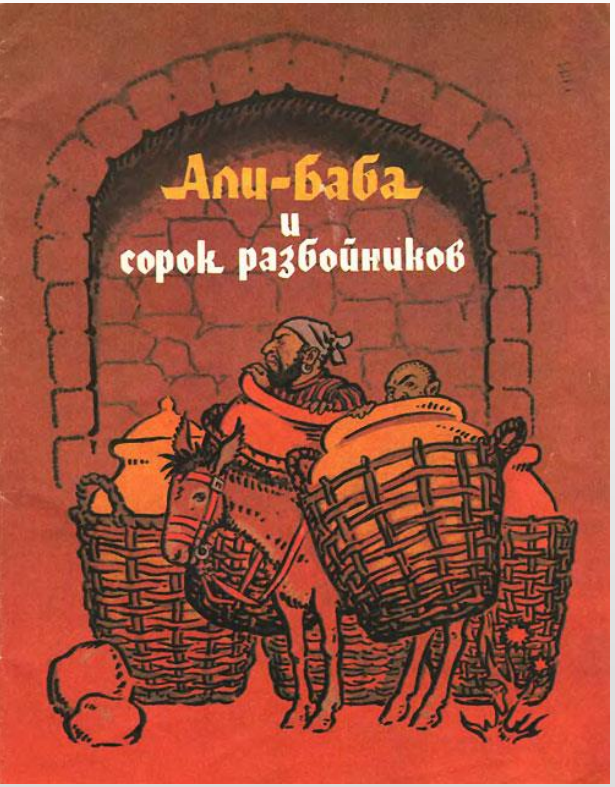
С древних времён перед людьми стояла довольно сложная задача — убедиться в достоверности важных сообщений. Придумывались речевые пароли, сложные печати. Появление методов аутентификации с применением механических устройств сильно упрощало задачу, например, обычный замок и ключ были придуманы очень давно.

Идентификация и аутентификация имеют разные функции. Первая предоставляет субъекту (пользователю или процессу, который действует от его имени) возможность сообщить собственное имя. При помощи аутентификации уже вторая сторона окончательно убеждается в том, что субъект действительно представляет собой того, за кого он себя выдает. Нередко в качестве синонимов идентификация и аутентификация заменяются словосочетаниями «сообщение имени» и «проверка подлинности»

В любой системе аутентификации обычно можно выделить несколько элементов:

- *субъект*, который будет проходить процедуру
- *характеристика* субъекта — отличительная черта
- *хозяин системы аутентификации*, несущий ответственность и контролирующий её работу
- сам *механизм аутентификации*, то есть принцип работы системы
- *механизм управления доступом*, предоставляющий определённые права доступа субъекту

ЭЦП. Элементы системы аутентификации



Элемент аутентификации	Пещера 40 разбойников	Регистрация в системе
Субъект	Человек, знающий пароль	Авторизованный пользов атель
Характеристика	Пароль "Сим-Сим, откройся!"	Тайный пароль
Хозяин системы	40 разбойников	Предприятие, которому принадлежит система
Механизм аутентификации	Волшебное устройство, реагирующее на слова	Программное обеспечение, проверяющее пароль
Механизм управления доступом	Механизм, отодвигающий камень от входа в пещеру	Процесс регистрации, управления доступом

Аутентификация и идентификация. Пароли

Главное достоинство парольной аутентификации - простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности.

Недостатки парольной идентификации:

- пароли не хранятся в тайне, имеют стандартные значения, указанные в документации, и далеко не всегда после установки системы производится их смена;
- ввод пароля можно подсмотреть - иногда для подглядывания используются даже оптические приборы;
- пароли нередко сообщают коллегам
- пароль можно угадать «методом грубой силы», используя, скажем, словарь, если файл паролей зашифрован, но доступен для чтения, его можно скачать к себе на компьютер и попытаться подобрать пароль, запрограммировав полный перебор (предполагается, что алгоритм шифрования известен).

Аутентификация и идентификация. Биометрия

Биометрия включает в себя комбинацию автоматизированных средств идентификации/аутентификации людей, основанную на их поведенческих или физиологических характеристиках. Физические средства аутентификации и идентификации предусматривают проверку сетчатки и роговицы глаз, отпечатков пальцев, геометрии лица и рук, а также другой индивидуальной информации. Поведенческие же характеристики включают в себя стиль работы с клавиатурой и динамику подписи. Комбинированные методы представляют собой анализ различных особенностей голоса человека, а также распознавание его речи.

В преимущественном большинстве случаев биометрия используется в комбинации с другими аутентификаторами наподобие интеллектуальных карт. Нередко биометрическая аутентификация представляет собой только первый рубеж защиты и выступает в качестве средства активизации интеллектуальных карт, включающих в себя различные криптографические секреты. При использовании данной технологии биометрический шаблон сохраняется на этой же карте

ЕСИА

Единая система идентификации и аутентификации (ЕСИА) — информационная система в Российской Федерации, обеспечивающая санкционированный доступ участников информационного взаимодействия (граждан-заявителей и должностных лиц органов исполнительной власти) к информации, содержащейся в государственных информационных системах и иных информационных системах.

Условно ЕСИА можно назвать «электронным паспортом» гражданина РФ. С её помощью происходит авторизация на таких сайтах как Госуслуги и Российская общественная инициатива.

Для получения учётной записи ЕСИА необходимо удостоверить свою личность с помощью паспортных данных, ИНН и СНИЛС.

Основные функции и задачи ЕСИА

Сеченовский Университет
наук о жизни

Функции

- идентификация и аутентификация пользователей
- управление идентификационными данными
- авторизация уполномоченных лиц органов исполнительной власти при доступе к функциям ЕСИА
- ЕСИА передает в МИС утверждение о пользователе
- ведение информации о полномочиях пользователей в отношении информационных систем

Задачи

- Предоставление пользователю единой учетной записи, которая дает возможность пользователю получить доступ к множеству значимых государственных информационных систем с использованием единой учетной записи
- Доступ различных категорий пользователей (например, физических лиц, представителей юридических лиц, индивидуальных предпринимателей) к информации, содержащейся в государственных информационных системах, муниципальных информационных системах и иных информационных системах.
- Взаимодействия информационных систем, то есть механизмов идентификации, аутентификации и авторизации информационных систем при взаимодействии с использованием СМЭВ

ЕСИА

Выполнив эти действия, Вы сможете создать учетную запись юридического лица или индивидуального предпринимателя

*Создать учетную запись юридического лица можно только из подтвержденной учетной записи физического лица – руководителя организации или представителя юридического лица, имеющего право действовать от имени организации без доверенности.

ЕСИА

Портал единой системы идентификации и аутентификации предусматривает три основных уровня учетных записей для физических лиц:

Упрощенная. Для ее регистрации достаточно просто указать свою фамилию и имя, а также какой-то определенный канал коммуникации в виде адреса электронной почты или мобильного телефона. Это первичный уровень, с помощью которого у человека открывается доступ только к ограниченному перечню различных государственных услуг, а также возможностей существующих информационных систем.

Стандартная. Для ее получения изначально нужно оформить упрощенную учетную запись, а потом уже предоставить также дополнительные данные, включая информацию из паспорта и номер страхового индивидуального лицевого счета. Указанная информация автоматически проверяется через информационные системы Пенсионного фонда, а также Федеральную миграционную службу, и, если проверка проходит успешно, учетная запись переводится на стандартный уровень, что открывает пользователю расширенный перечень государственных услуг.

Подтвержденная. Для получения такого уровня учетной записи единая система идентификации и аутентификации требует от пользователей стандартный аккаунт, а также подтверждение личности, которое выполняется через личное посещение отделения уполномоченной службы или посредством получения кода активации через заказное письмо. В том случае, если подтверждение личности окажется успешным, учетная запись перейдет на новый уровень, а перед пользователем откроется доступ к полному перечню необходимых государственных услуг.

Этапы интеграции МИС с ЕСИА

Сеченовский Университет
наук о жизни

Организационный этап

- Определить ответственного за эксплуатацию информационной систем
- Зарегистрировать ответственного человека в ЕСИА и пройти процедуру подтверждения личности
- Создать учетную запись организации через портал Госуслуг. Получить КЭЦП (http://minsvyaz.ru/ru/appeals/faq/35/)
- Зарегистрировать МИС через технологический портал (http://esia.gosuslugi.ru/console/tech).

Регистрация информационной системы в Министерстве связи

Технический этап

- Генерация закрытого ключа и сертификата открытого ключа для МИС.
- Формируем файл метаданных на основе сертификата открытого ключа
- Оформляем заявку на подключение МИС к тестовой среде ЕСИА.
- Разработать или приобрести модуль авторизации ЕСИА для МИС
- Встроить модуль ЕСИА и произвести отладку для обеспечения процедуры формирования и отправки запросов
- Отравить заявку на подключение к промышленной среде ЕСИА

Подключение информационной системы к ЕСИА.

Эксплуатация

- Промышленная эксплуатация МИС с возможностью сквозной аутентификации через портал ЕСИА

Использование ЕСИА

Сквозная аутентификация в МИС с использованием портала ЕСИА

Сеченовский Университет
наук о жизни

Браузер пользователя

HTTPS
Saml 2.0

HTTPS
Saml 2.0

Медицинская информационная система

Пользователь обращается к МИС

МИС перенаправляет пользователя в ЕСИА

Пользователь проходит аутентификацию в ЕСИА

ЕСИА передает в МИС утверждение о пользователе

Пользователь попадает в МИС

Вредоносное программное обеспечение

На жаргоне некоторых специалистов «*вирус*», англ. *malware*, *malicious software* — «злонамеренное программное обеспечение») — любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с целью несанкционированного использования ресурсов ЭВМ или причинения вреда (нанесения ущерба) владельцу информации, и/или владельцу ЭВМ, и/или владельцу сети ЭВМ, путём копирования, искажения, удаления или подмены информации. Многие антивирусы считают крэки(кряки), кейгены и прочие программы для взлома приложений вредоносными программами, или потенциально опасными

Согласно статье 273 Уголовного Кодекса Российской Федерации(«Создание, использование и распространение вредоносных компьютерных программ») определение вредоносных программ выглядит следующим образом: «… заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации…»

Вредоносное программное обеспечение. Классификация

- классические компьютерные вирусы (Vuruses);
- сетевые черви (Worms);
- троянские программы (Trojans);
- программы-шпионы (Spy Ware);
- логические бомбы (Logic Bomb);
- архивные бомбы;
- почтовые (кластерные) бомбы;
- хакерские утилиты;
- другие программы, наносящие заведомый вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в сети.

Компьютерные вирусы

Вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.

Основная цель вируса — его распространение, а нарушение работы программно-аппаратных комплексов — удаление файлов, приведение в негодность структур размещения данных, блокирование работы пользователей и т. п. — часто является его сопутствующей функцией.

Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами. Кроме того, вирусы, как правило, занимают место на накопителях информации и потребляют ресурсы системы.

В обиходе «вирусами» называют всё вредоносное ПО, хотя на самом деле это лишь один его вид.

Основы теории самовоспроизводящихся механизмов заложил американец венгерского происхождения Джон фон Нейман, который в 1951 году предложил метод создания таких механизмов. С 1961 года известны рабочие примеры таких программ.

Первыми известными вирусами являются Virus 1,2,3 и Elk Cloner для ПК Apple II, появившиеся в 1981 году. Зимой 1984 года появились первые антивирусные утилиты CHK4BOM и BOMBSQAD авторства Энди Хопкинса . В начале 1985 года Ги Вонг написал программу DPROTECT — первый резидентный антивирус.

Свойства компьютерных вирусов

Обязательным (необходимым) свойством компьютерного вируса является возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.

Разновидностей вирусов, различающихся по основному способу распространения и функциональности. Если изначально вирусы распространялись на дискетах и других носителях, то сейчас доминируют вирусы, распространяющиеся через локальные и глобальные (Интернет) сети. Растёт и функциональность вирусов, которую они перенимают от других видов программ.

Классификация компьютерных вирусов № 1

Сеченовский Университет
наук о жизни

В настоящее время не существует единой системы классификации и именования вирусов (хотя попытка создать стандарт была предпринята на встрече CARO в 1991 году). Принято разделять вирусы:

- по поражаемым объектам (файловые вирусы, загрузочные вирусы, сценарные вирусы, макровирусы);
- файловые вирусы делятся по механизму заражения: паразитирующие добавляют себя в исполняемый файл, перезаписывающие невосстановимо портят заражённый файл, «спутники» идут отдельным файлом.
- по поражаемым операционным системам и платформам (DOS, Windows, Unix, Linux, Android);
- по технологиям, используемым вирусом (полиморфные вирусы, стелс-вирусы, руткиты);
- по языку, на котором написан вирус (ассемблер, высокоуровневый язык программирования);
- по дополнительной вредоносной функциональности (бэкдоры, кейлоггеры, шпионы, ботнеты и др.).

Классификация компьютерных вирусов № 2

Сеченовский Университет
наук о жизни

Среда обитания	Заражаемая операционная система	Особенности алгоритма	Деструктивные возможности
❑ файловые; ❑ загрузочные; ❑ макро; ❑ сетевые.	❑ DOS; ❑ Windows; ❑ Unix ❑ Linux ❑ Android ❑ IOS	❑ резидентность; ❑ использование стелс-алгоритмов; ❑ самошифрование полиморфичность ❑ метаморфичность	❑ безвредные, ❑ неопасные, ❑ опасные вирусы ❑ очень опасные

Метаморфные, загрузочные и макро-вирусы

Метаморфные вирусы, так же изменяют свой код, но не используют алгоритмы шифрования. Различие проявляется в виде изменений внутри кода вируса. Существует несколько технологий, позволяющих с успехом реализовывать данную методику. Одна из этих технологий трансформации, используемая метамофными программами основана на вставке и удалении«мусора» внутри кода.

Принцип действия **загрузочных вирусов** основан на алгоритмах запуска операционной системы при включении или перезагрузке компьютера - после необходимых тестов установленного оборудования (памяти, дисков и т.д.) программа системной загрузки считывает первый
физический сектор загрузочного диска и передает на него управление.

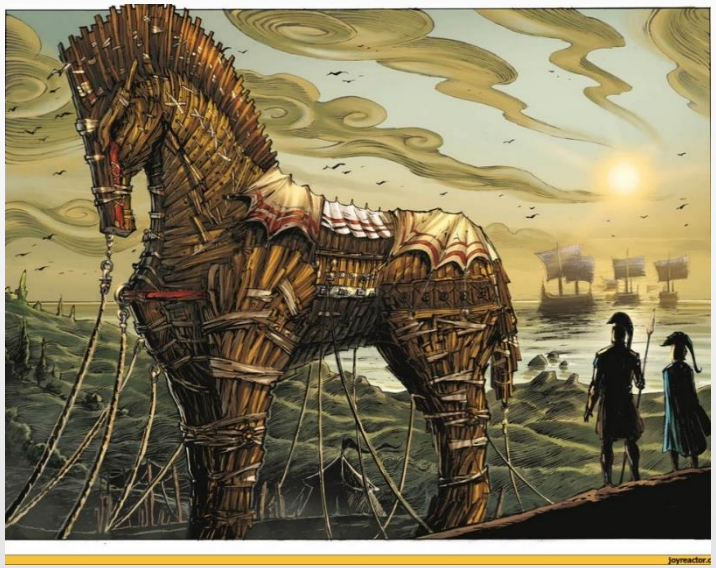
Макро-вирусы являются программами на языках, встроенных в некоторые системы обработки данных(текстовые редакторы, электронные таблицы и т.д.). Для своего размножения такие вирусы используют возможности макро-языков и при их помощи переносят себя из одного зараженного файла(документа или таблицы) в другие. Для существования вирусов в конкретной системе (редакторе) необходимо наличие встроенного в систему макро-языка с возможностями:

Сетевые, почтовые, пиринговые и файловые вирусы

Сетевые черви, для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию и захватить управление. Для внедрения в заражаемую систему червь может использовать различные механизмы: дыры, слабые пароли, уязвимости базовых и прикладных протоколов, открытые системы и человеческий фактор.

Вирус пиринговых сетей— это вредоносная программа, специально предназначенная для систем обмена файлами между компьютерами пользователей Интернета, такими как Windows Messenger, ICQ и т.д. Чтобы такой вирус попал на компьютер пользователя пиринговой сети, пользователю требуется выполнить какое либо действие, например, загрузить и запустить на выполнение файл.

Программные закладки



Резидентные

Не Резидентные

Три типа программных закладок:

- вносить произвольные искажения в коды программ, находящихся оперативной памяти компьютера (например, внесение изменений в программу разграничения доступа может привести к тому, что она разрешит вход в систему всем без исключения пользователям вне зависимости от правильности введенного пароля) -программная закладка первого типа;

- копировать фрагменты информации (пароли, криптографические ключи, коды доступа, конфиденциальные электронные документы и др.), из одних областей оперативной или внешней памяти компьютера в другие- программная закладка второго типа;

- искажать выводимую на внешние компьютерные устройства или в канал связи информацию, полученную в результате работы других программ- программная закладка третьего типа.

Важная особенность - обязательно выполняют операцию записи в оперативную или внешнюю память системы. При отсутствии данной операции никакого негативного влияния программная закладка оказать не может.

Модели воздействия программных закладок на компьютеры

Перехват - В модели перехват программная закладка внедряется в ПЗУ, системное или прикладное программное обеспечение и сохраняет всю или выбранную информацию, вводимую с внешних устройств компьютерной системы или выводимую на эти устройства, в скрытой области памяти локальной или удаленной компьютерной системы. Объектом сохранения, например, могут служить символы, введенные с клавиатуры, или электронные документы, распечатываемые на принтере.

Искажение - В модели искажение программная закладка изменяет информацию, которая записывается в память компьютерной системы в результате работы программ, либо подавляет/инициирует возникновение ошибочных ситуаций в компьютерной системе.

Удаление информации

Наблюдение и компрометация - Помимо перечисленных, существуют и другие модели воздействия программных закладок на компьютеры. В частности, при использовании модели типа наблюдение программная закладка встраивается в сетевое или телекоммуникационное программное обеспечение. Пользуясь тем, что подобное программное обеспечение всегда находится в состоянии активности, внедренная в него программная закладка может следить за всеми процессами обработки информации в компьютерной системе, а также осуществлять установку и удаление других программных закладок.

Утилиты скрытого администрирования, Fishing, Spyware, Adware, Клавиатурные шпионы

Сеченовский Университет
наук о жизни

Утилиты скрытого администрирования(backdoor) Троянские программы этого класса по своей сути является достаточно мощными утилитами удаленного администрирования компьютеров в сети. По своей функциональности они во многом напоминают различные системы администрирования, разрабатываемые и распространяемые различными фирмами-производителями программных продуктов. Но только в случаи преднамеренной установки например системным администратором, утилиту можно считать не вредоносной.

Техника Fishing используется с целью выманить у пользователя Интернета персональную информацию(пароли, пин-коды и т.д.). При этом злоумышленники могут направлять ему поддельные сообщения электронной почты. В этих сообщениях, отправленных, например, от имени популярногоWeb-сайта или банка, может говориться о том, что по той или иной причине пользователь должен выслать банку пароль или пин-код.

Программы Spyware устанавливаются на компьютер пользователя и собирают различную информацию о действиях пользователя. Обычно это информация, енная для маркетологов, которая после сбора отсылается разработчику программы через Интернет.

Программы Adware отображают рекламную информацию на компьютере. Эти программы могут отображать на экране всплывающие окна с рекламными баннерами и текстом, даже при отсутствии подключения к Интернету.

Руткиты, Клавиатурный шпион, Логическая бомба, Зобми компьютер , Ботнет, Пугающие или вымогающие, Скрытые индикаторы

Сеченовский Университет
наук о жизни

Руткит (Rootkit) это скрытый тип вредоносного программного обеспечения, который выполняется на уровне ядра операционной системы. Основной опасностью руткитов является то, что, внедряясь на уровень ядра системы, руткиты могут выполнять любые действия и с легкостью обходить любые системы защиты, ведь для своего скрытия им достаточно отказать в доступе средствам безопасности. Кроме того, руткиты позволяют скрывать действия других вредоносных программ. Обычно, их применяют для удаленного контроля компьютера.

Зобми - Программы для создания из вашего компьютера зомби предназначены для внедрения на компьютер кода, который, подобно, логической бомбе, будет активироваться при определенных условиях (обычно, речь идет об удаленном доступе - отсылке команд). При заражении компьютера, чаще всего применяются троянские программы. В последствии, зомбированный компьютер используется для рассылки спама, проведения DDoS атак (распределенная атака в обслуживании), накрутки счетчиков и прочих вредоносных действий, без ведома владельца.

Ботнет - Часто, зомби компьютеры организуются в сеть, называемую ботнет (botnet). В такой сети часть компьютеров представляет собой ретрансляторы для передачи команды от удаленного компьютера злоумышленника на все зомбированные узлы. Это позволяет злоумышленникам легко управлять ботнет сетями, измеряемыми в десятках и сотнях тысяч. Как правило, такие сети используют для проведения согласованных вредоносных действий в интернете, без ведома владельцев зараженных компьютеров.

Ботнеты. Скрытый майнинг.

Сеченовский Университет
наук о жизни

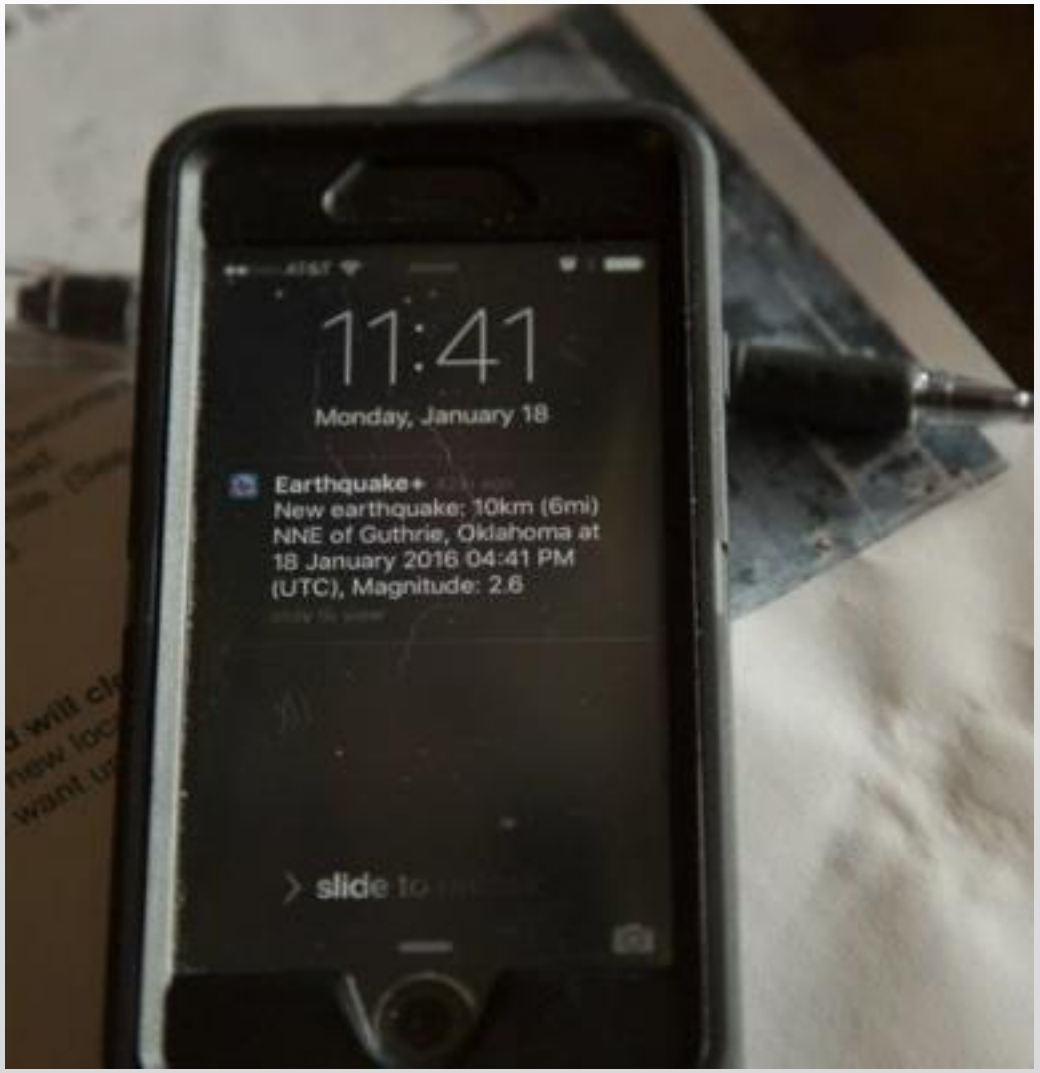
В тайне от пользователя, например, при открытии любого файла, ему устанавливается программа-клиент, которая подключается к одному из майнинг-пулов и начинает добывать криптовалюту.

Заражение происходит различными способами:

- Через любые запущенные файлы;
- Прямой подсадкой на ПК (редкость);
- Посредством несанкционированного удалённого доступа.

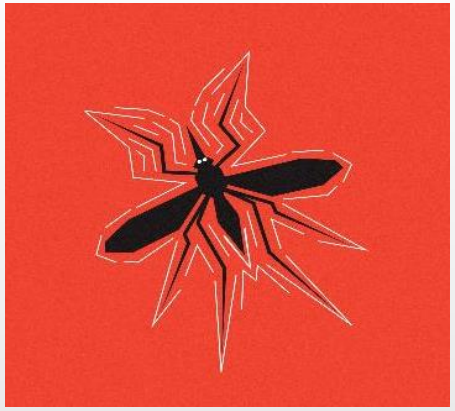
Самый известный случай – попытка разработчиков µTorrent таким образом дополнительно заработать на пользователях внедрив в софт скрытый майнер EpicScale.

Сети LTE и уязвимости



Исследователи из Purdue и Университета штата Айова описали эксплойты в протоколах LTE, которые позволили бы злоумышленникам совершить десять типов серьезных атак, в том числе перехват вызовов и текстовых сообщений, отслеживание местоположения, отключение устройства в автономном режиме и даже подделка экстренных предупреждений. Хакеры могут воспользоваться тремя ключевыми задачами протокола (например, подключением устройства к сети и поддержанием соединения) для проведения атак с использованием ретрансляции, которые не только позволяют подключаться к сети без учетных данных, но и маскироваться под устройство жертвы.

Извлечение данных с помощью наушников



Команда исследователей из Университета имени Бен-Гуриона (Израиль) разработала новый метод для извлечения данных с физически изолированных компьютеров с помощью колонок и наушников, получившая название MOSQUITO

Метод предполагает использование техники, известной как jack retasking (переназначение аудиоразъемов), что позволяет эффективно превратить динамик в микрофон.

Вредоносное ПО, установленное на физически изолированном компьютере, может преобразовывать локальные файлы в аудиосигналы и передавать их на другой компьютер через подключенные колонки или наушники.

Далее второй компьютер, также зараженный вредоносным ПО, с помощью техники jack retasking превращает колонки или наушники в микрофон, получает модулированный сигнал и конвертирует его в обратно в файл данных.

Специалисты разработали протокол, модулирующий двоичные данные в аудиосигналы, и протестировали атаку на расстоянии от 1 до 9 метров. Скорость передачи данных с компьютера на компьютер варьировалась от 1800 бит/с до 1200 бит/с в эксперименте, когда колонки находились напротив друг друга и издавали звук в слышимом для человека диапазоне (ниже 18 кГц).

Основные средства защиты информации (СЗИ)
Антивирус

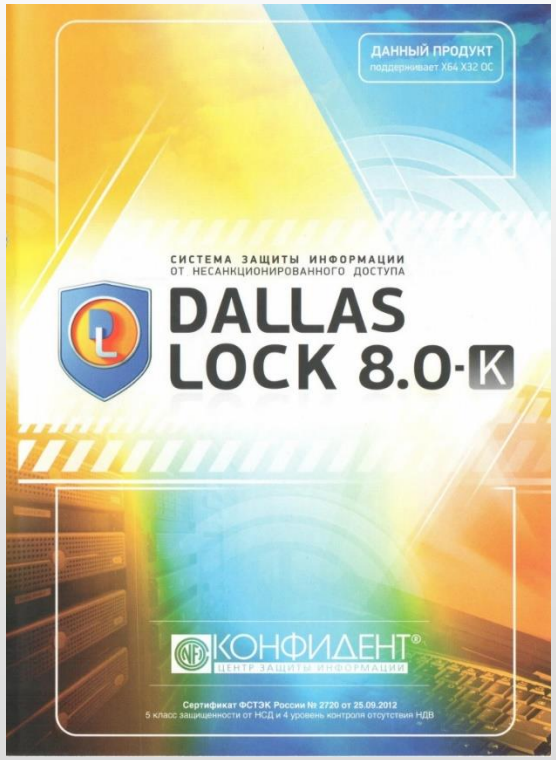
Антивирусные программы - современные антивирусные программы обеспечивают комплексную защиту программ и данных на компьютере от всех типов вредоносных программ и методов их проникновения на компьютер: Интернет, локальная сеть, электронная почта, съемные носители информации. Для защиты от вредоносных программ каждого типа в антивирусе предусмотрены отдельные компоненты. Принцип работы антивирусных программ основан на проверке файлов, загрузочных секторов дисков и оперативной памяти и поиске в них известных и новых вредоносных программ.

Антивирусное программное обеспечение

Антивирусное ПО может использовать следующие методы обнаружения вирусов и других вредоносных программ:

- сканирование;
- эвристический анализ(блокирование подозрительных действий)
- CRC-сканирование(обнаружение изменений);
- анализ сетевого трафика;
- анализ баз данных почтовых программ;
- обнаружение вирусов в системе автоматизации документооборота.
- информацию о содержании жесткого диска с елью составления списка ПО, установленного на компьютере у пользователя;
- информацию о нажатых клавишах(клавиатурные шпионы);
- приложения, с которыми работает пользователь;
- сведения о посещении Web-сайтов и другой активности в Интернете;
- содержимое сообщений электронной почты

Основные средства защиты информации (СЗИ) Средства от Несанкционированного доступа.



Несанкционированный доступ к информации (НСД) — это доступ к данным, который нарушает правила разграничения доступа с реализацией определенных средств которые являются средствами вычислительной техники или автоматизированными системами.

Основные средства защиты информации (СЗИ)
Средства от Несанкционированного доступа.

Управление доступом.
Протоколирование и аудит.

Шифрование.

Экранирование.

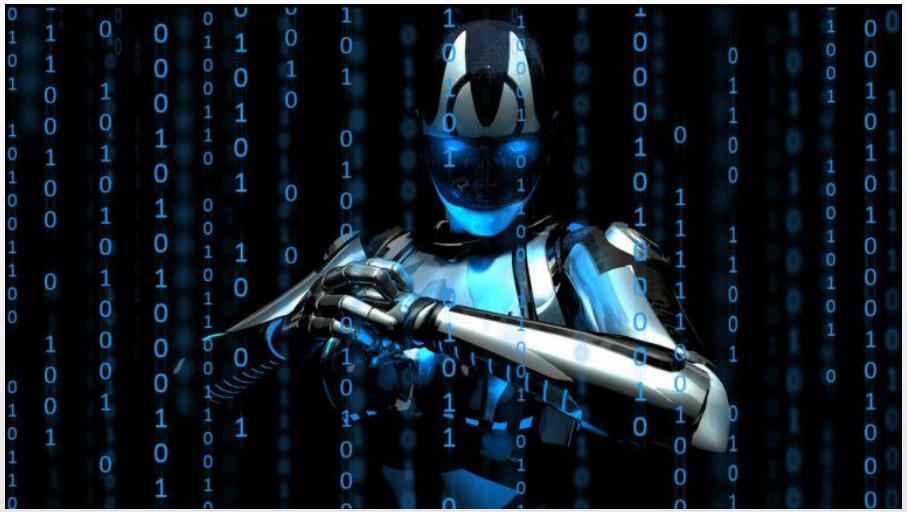
Туннелирование.

Контроль целостности.

Контроль защищенности.

Обнаружение отказов и операти
восстановление.
Управление.

Методы борьбы и профилактики



Алгоритм работы - Обязательно использовать комплексный подход.

1. **Утилита AnVir Task Manager** – выявляем скрытые или подозрительные процессы. (Удалить все ненужное для работы операционной системы)
2. **ProcessExplorer**- позволяет обнаружить процессы **именно** загружающие процессор.
3. Переходим в **Безопасный режим**

4. **Запускаем утилиты** Web CureIt! /Kaspersky Virus Removal Tool/COMODO Cleaning Essentials/ Junkware Removal Tool/AdwCleaner - **анализируем результаты**
5. Применение **AVZ** и форума **VirusInfo** (https://virusinfo.info/) Запускаем «Исследование системы» и получаем файл avz_sysinfo.htm.
6. **Очистка реестра** CCLeaner /AuslogicBootSpeed.
7. Если все эти пункты не помогли, придется готовится к **переустановке операционной системы.**

Литература

1. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В Основы криптографии.
2. Бабаш А.В, Шанкин Г.П. Критпография. Под редакцией В.П. Шерстюка, Э.А. Применко/ А.В. Бабаш, Г.П. Шанкин. – М.: СОЛОН_ПРЕСС, 2007. – 512 с., ил. – (Серия книг«Аспекты защиты»).
3. Блейхут Р. Теория и практика кодов, контролирующих ошибки= Theory and Practice of Error Control Codes. – М.: Мир, 1986. – 576 с.
4. Венбо Мао Современная криптография. Теория и практика– М.:Вильямс, 2005. – 768 с. – 2 000 экз. – ISBN 5–8459–0847–7, ISBN 0–13–066943–1
5. Герасименко В.А., Малюк А.А. Основы защиты информации. – М.: МГИФИ, 1997.
6. Грушо А.А., Применко Э.А., Тимонина Е.Е. Анализ и синтез криптоалгоритмов. Курс лекций. Москва2000.
7. Дадуков, Н.С. Советская шифровальная техника[Текст]: ленинградский период: 1935-1941 / Н. С. Дадуков[и др.] // Защита информации. Инсайд. – 2006. – N 1. – С. 91-96. – 2006.
8. Дональд Э. Кнут Глава3. Случайные числа// Искусство программирования. – 3–е изд. – М.: Вильямс, 2000. – Т. 2. Получисленные алгоритмы. – 832 с. – ISBN 5–8459–0081– 6
9. Жельников В. Криптография от папируса до компьютера. М.: ABF, 1996. 336 с.
10. Зима В.М., Молдовян А.А., Молдовян Н.А. Компьютерные сети и защита передаваемой информации. – СПб.: СПбГУ, 1998.
11. Иванов М.А., Чугунков И.В. Глава4. Методика оценки качества генераторов ПСП// Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: КУДИЦ–ОБРАЗ, 2003. – 240 с. – ISBN 5–93378–056–1 139
12. Исагулиев К.П. Справочник по криптологии. – Минск: Новое издание, 2004.–237с. ISBN 985–475–079–5.
13. Корн Г., Корн Т. Справочник по математике(для научных работников и инженеров). Пер. с англ./ Под ред. И.Г. Арамановича. М.: Наука, 1973. 832 с.
14. Леонов А.П., Леонов К.П., Фролов Г.В. Безопасность автоматизированных банковских и офисных технологий. – Мн.: Нац. кн. палата Беларуси, 1996.
15. Математические и компьютерные основы криптологии: Учебное пособие/ Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич. – Минск: Новое издание, 2003. –382с. ISBN 985–475–016–7.
16. Мельников В.В. Защита информации в компьютерных системах. – М.: Финансы и статистика, 1997.
17. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. М.: ЛАЙТ Лтд., 2002.
18. Романец Ю.В., Тимофеев П. А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 1999.
19. Ростовцев А.Г., Маховенко Е.Б. Теоретическая критптография. АНО НПО«профессионал», СПб2004
20. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. – Москва. – Изд-во Горяч. Линия-Телеком, 2005. – ISBN 5–93517–265–8.
21. Саломаа А. Криптография с открытым ключом. Пер. с англ. – М.: Мир, 1995. – 318 с., ил.
22. Смарт Н. Криптография. Серия«Мир программирования». Пер. с англ. С.А. Кулешова/ Под ред. С.К. Ландо. М.: Техносфера, 2005. 528 с.
23. Теория электрической связи: учебное пособие/ К.К. Васильев, В.А. Глушков, А.В. Дормидонтов, А.Г. Нестеренко; под общ. ред. К.К. Васильева. – Ульяновск: УлГТУ, 2008. – 452 с.
24. Фороузан Б.А.Схема цифровой подписи Эль-Гамаля// Управление ключами шифрования и безопасность сети/ Пер. А. Н. Берлин– Курс лекций. 140
25. Х.К.А. Ван Тилборг. Основы криптологии. Профессиональное руководство и интерактивный учебник. – М.: Мир, 2006, стр. 471
26. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си– М.: Триумф, 2002. – С. 446-448. – 816 с. – 3000 экз. – ISBN 5–89392–055–4.
27. Menezes, P. van Oorschot, S. Vanstone Handbook of Applied Cryptography. – CRC Press, Inc. – 1997.
28. ГОСТ Р34.10-2001. Информационные технологии. Криптографическая защита информации. Процессы формирования и проверки цифровой подписи.
29. Гатченко Н.А., Исаев А.С., Яковлев А.Д. «Криптографическая защита информации» – СПб: НИУ ИТМО, 2012. – 142 с.

Сеченовский Университет
наук о жизни

Спасибо за внимание!

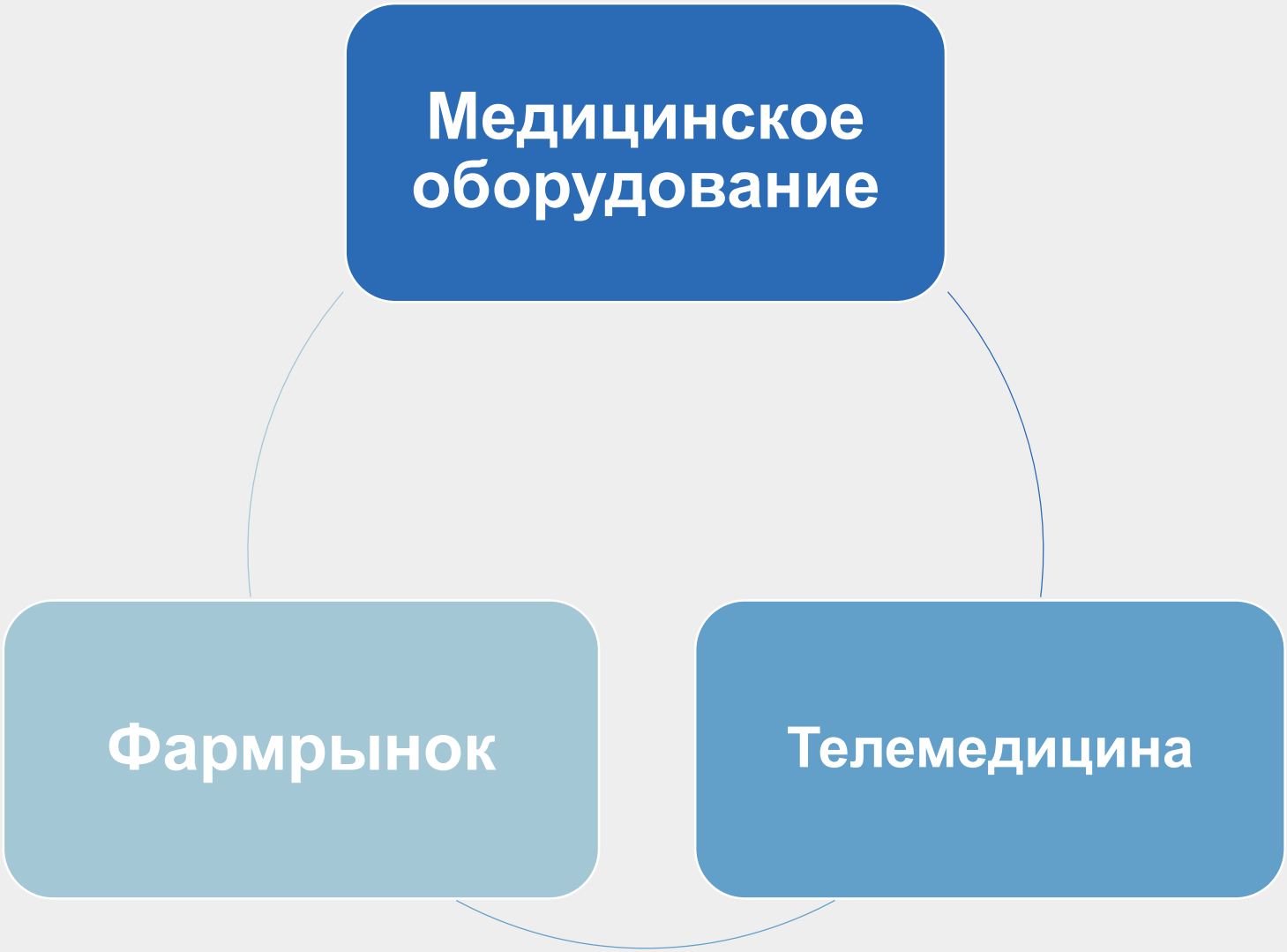
Рябков Илья Валерьевич
Старший преподаватель

Телемедицина

Шадёркин Игорь Аркадьевич

Заведующий лабораторий электронного здравоохранения Института цифровой медицины ФГАОУ ВО Первый МГМУ имени И.М. Сеченова Минздрава России (Сеченовский Университет)

2.1. Возможности телемедицины


Медицинское оборудование
Фармрынок
Телемедицина

Что такое телемедицина?

- Дистанционное **образование**
- **Организация** медицинской помощи
- Поддержка клинических **исследований**
- **Клиническая** телемедицина
  - mHealth

Телемедицинские технологии – информационные технологии, обеспечивающие дистанционное взаимодействие медицинских работников между собой, с пациентами и (или) их законными представителями, идентификацию и аутентификацию указанных лиц, документирование совершаемых ими действий **при проведении консилиумов, консультаций, дистанционного медицинского наблюдения** за состоянием здоровья пациента

323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»

Трехуровневая система

Онлайн анкетирование

Международная система оценки сим простаты IPSS

У Вас имеется средняя степень недомогания, т.е. ес
Вашей ситуации, желательно обратиться к урологу.

Вернуться к списку тестов

Задать вопрос урологу

https://nethealth.ru/

Анкеты

Анкета вероятности рецидива МКБ — Пройти тест

Анкета рассчитывает вероятность рецидива и развития МКБ

Анкета опроса питания для пациентов с МКБ — Пройти тест

Рацион питания в значительной степени определяет риски развития и рецидивирования мочекаменной болезни.

Заполнение данной анкеты позволит определить стереотип питания, на основе коррекции которого врач сформирует оптимальный рацион, направленный на предупреждение мочекаменной болезни.

Тесты

Международная система оценки симптомов болезни простаты IPSS — Пройти тест

Вы можете провести оценку своего урологического здоровья по "Международная система оценки симптомов болезни простаты IPSS"

Проверьте свой уровень ПСА — Пройти тест

Этот тест для пациентов, которые **впервые** сделали анализ на **ПСА** (**простатспецифический антиген**) и хотят узнать, что означают результаты в зависимости от уровня обнаруженного простатспецифического антигена.

Тест нарушения эрекции — Пройти тест

Пройдя этот тест, Вы сможете найти ответ на свой вопрос: "Есть ли у меня нарушения эрекции?".

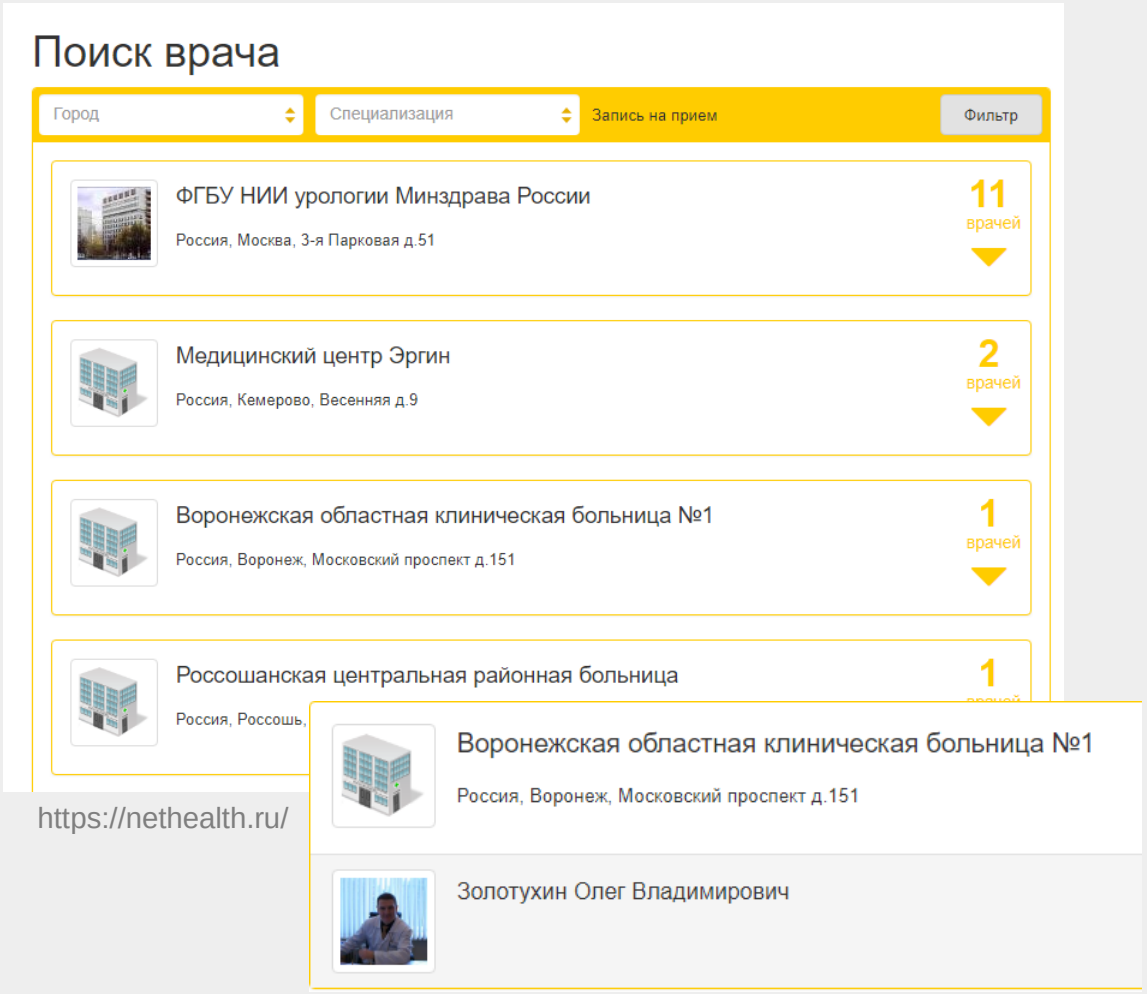
Международный индекс эректильной функции (IIEF) — Пройти тест

Пройдя этот тесты, Вы можете узнать имеются ли у Вас нарушения эрекции и какой степени они выраженности согласно "Международного индекса эректильной функции (IIEF)"

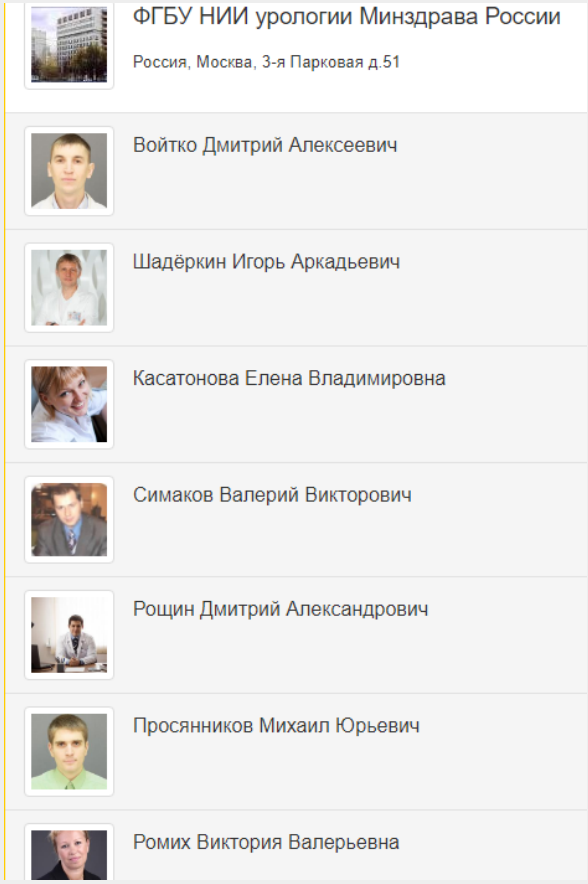
Размер полового члена — Пройти тест

Пройдя этот тест, Вы можете узнать информацию о **размере полового члена**.

Маршрутизация пациентов + лидогенерация



https://nethealth.ru/



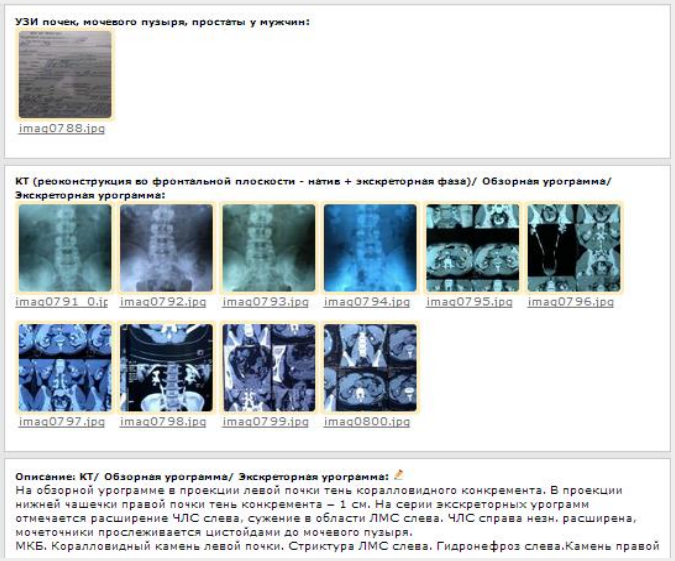
Телемедицинские консультации (пациент – врач)

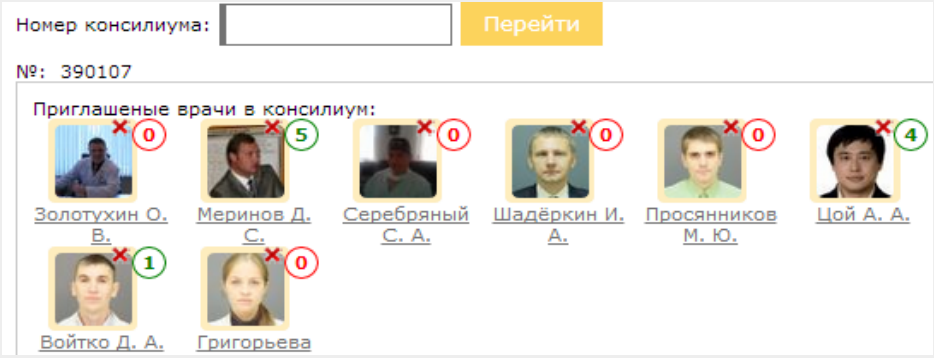
1. **Первичное** консультирование (первичный прием)
    1. **Профилактический** прием
    2. **Второе мнение** – назначение дополнительного обследования
2. **Вторичное** консультирование (вторичный прием)
    1. **Коррекция** назначенного ранее лечения
    2. **Мониторинг** – дистанционное наблюдение

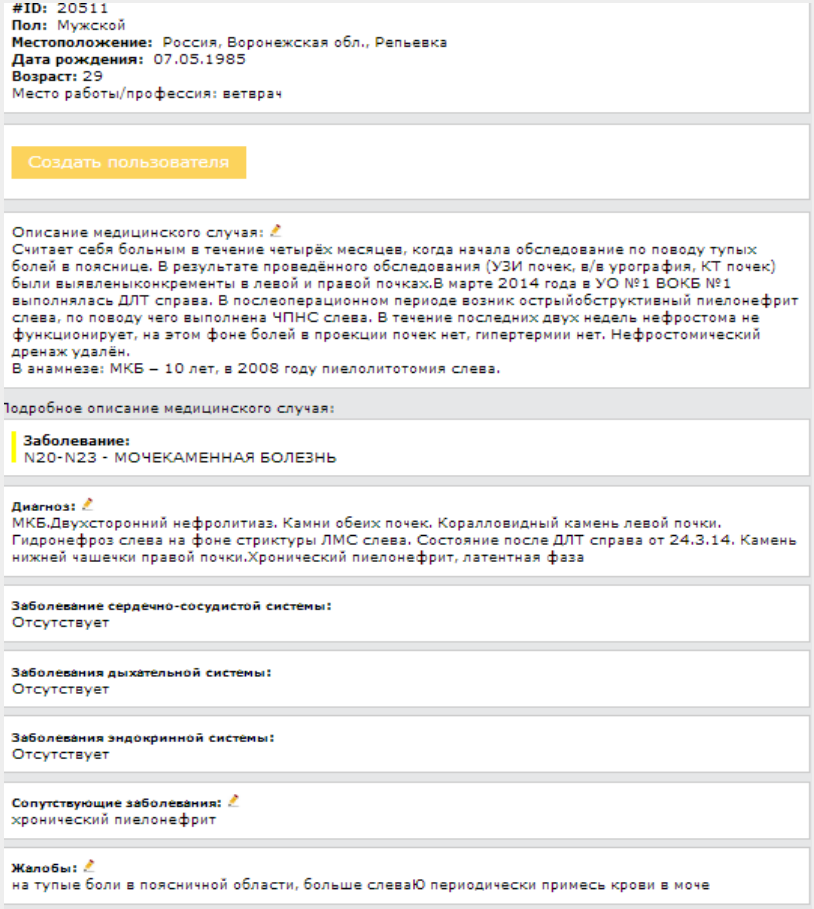
Дистанционное наблюдение

https://nethealth.ru/
http://ettagroup.ru/

Телемедицинские консилиумы

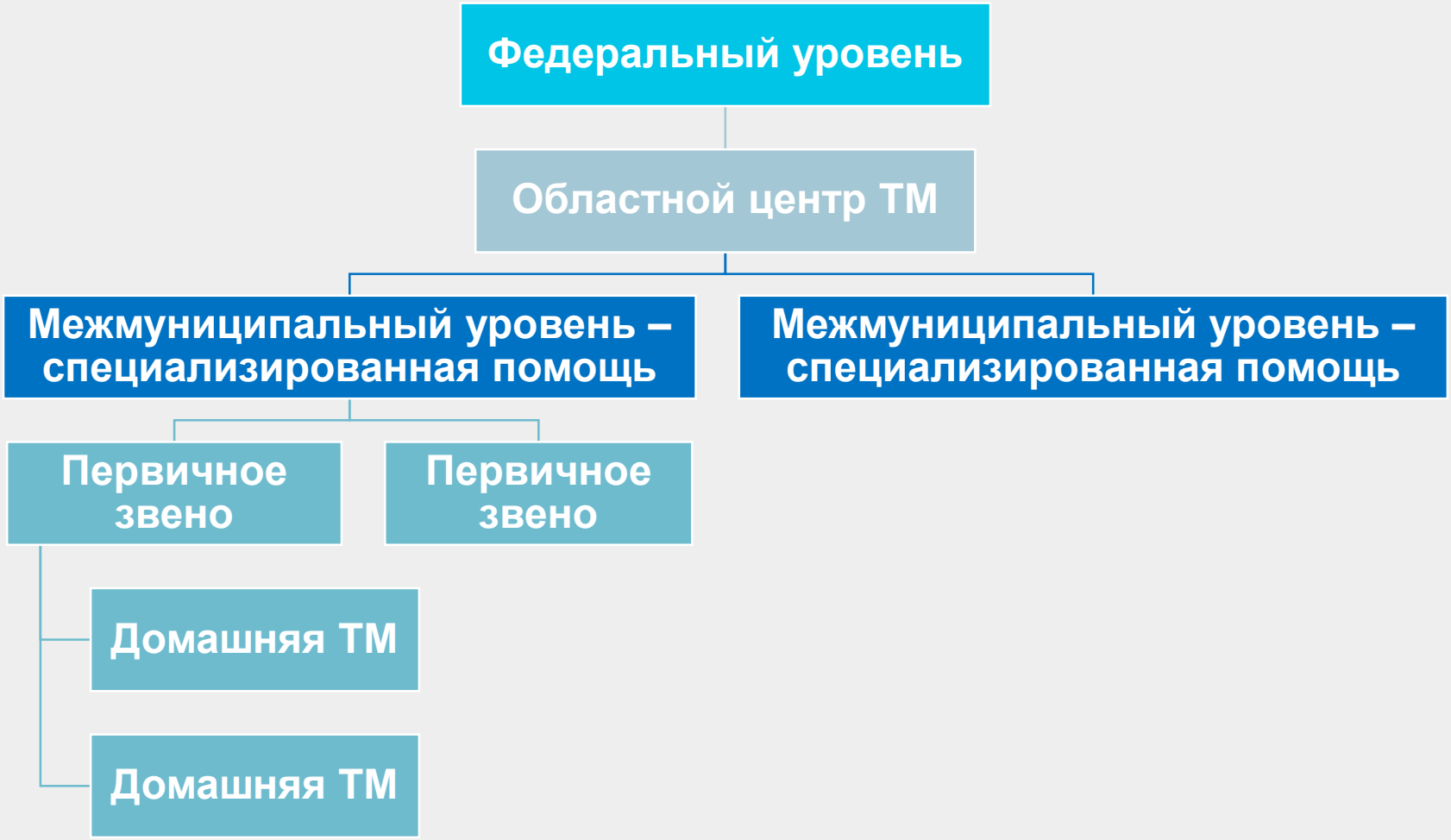






https://nethealth.ru/

Структура телемедицинской помощи в РФ



«Разработка научно обоснованной стратегии развития региональной системы охраны здоровья населения Сахалинской области на период до 2020 года» и «Исследование демографической ситуации в Сахалинской области, возможностей и мер по ее улучшению, включая развитие системы охраны репродуктивного здоровья населения на период до 2020 года». (Государственный контракт от 10 мая 2016 г. № 172)

2.2. Законодательное обеспечение телемедицины

Наиболее значимые нормативно-правовые акты в здравоохранении

- Конституция Российской Федерации.
- ФЗ от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» – основной закон в сфере здравоохранения
- ФЗ от 29.11.2010 г. № 326-ФЗ «Об обязательном медицинском страховании»
- ФЗ от 12.04.2010г. № 61-ФЗ «Об обращении лекарственных средств»
- ФЗ от 04.05.2011г. № 99-ФЗ «О лицензировании отдельных видов деятельности»
- Постановление Правительства РФ от 12 ноября 2012 г. N 1152 «Об утверждении положения о государственном контроле качества и безопасности медицинской деятельности»
- Постановление Правительства РФ от 25 сентября 2012 г. N 970 «Об утверждении Положения о государственном контроле за обращением медицинских изделий»
- Постановление Правительства РФ от 19 декабря 2015 г. № 1382 «О Программе государственных гарантий бесплатного оказания гражданам медицинской помощи на 2016 год»
- Приказы Министерства здравоохранения РФ – «Порядки оказания медицинской помощи населению Российской Федерации». Всего 60 Приказов/Порядков
- Приказы Министерства здравоохранения РФ – «Стандарты медицинской помощи». Эти приказы разбиты на 4 вида медицинской помощи (первичная медико-санитарная, специализированная, скорая и паллиативная), которые в себе содержат классы, привязанные к нозологическим единицам и группам заболевания согласно классификации МКБ-10. Всего порядка 1200 стандартов.

ФЗ 242 вступил в силу 1 января 2018 года

- Федеральный закон № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья»
- Документ вносит поправки в три Федеральных Закона:
  1. Федеральный закон от 8 января 1998 г. N 3-ФЗ «О наркотических средствах и психотропных веществах
  2. Федеральный закон от 12 апреля 2010 г. N 61-ФЗ «Об обращении лекарственных средств»
  3. Федеральный закон от 21 ноября 2011 г. N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»

Закон регулирует три основных направления в здравоохранении РФ

- Развитие Единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ)
- Электронный документооборот в здравоохранении, включая выписку электронных рецептов, в том числе на наркотики и сильнодействующие психотропные средства
- Оказания медицинской помощи с применением телемедицинских технологий

«Закон о телемедицине»

Определение телемедицинских технологий

Статья 2 пункт 22) **телемедицинские технологии** – информационные технологии, обеспечивающие дистанционное взаимодействие медицинских работников между собой, с пациентами и (или) их законными представителями, идентификацию и аутентификацию указанных лиц, документирование совершаемых ими действий при проведении консилиумов, консультаций, дистанционного медицинского наблюдения за состоянием здоровья пациента

Федеральный закон от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»

Статья 10. Доступность и качество медицинской помощи

Доступность и качество медицинской помощи обеспечиваются:

10) применением телемедицинских технологий

Федеральный закон от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»

Информированное добровольное согласие

Статья 20 часть 7. **Информированное добровольное согласие** на медицинское вмешательство или отказ от медицинского вмешательства… оформляется в виде документа на бумажном носителе…, либо формируется **в форме электронного документа**, подписанного… с использованием **усиленной квалифицированной электронной подписи** или простой **электронной подписи посредством применения единой системы идентификации и аутентификации**, а также медицинским работником с использованием усиленной квалифицированной электронной подписи…

Федеральный закон от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»

Запрос медицинских документов

Статья 22 часть 5. Пациент либо его законный представитель имеет право по запросу, направленному в том числе **в электронной форме**, получать отражающие состояние здоровья пациента медицинские документы (их копии) и выписки из них, в том числе **в форме электронных документов**

Федеральный закон от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»

Статья 36.2. Особенности медицинской помощи, оказываемой с применением телемедицинских технологий

Федеральный закон от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»

Порядки и стандарты при применении ТМ технологий

Медицинская помощь с применением телемедицинских технологий организуется и оказывается в **порядке (1)**, установленном уполномоченным федеральным органом исполнительной власти, а также **в соответствии с порядками (2)** оказания медицинской помощи и на основе **стандартов медицинской помощи (3)**

Федеральный закон от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»

Первичная консультация

2. **Консультации** пациента или его законного представителя медицинским работником с применением телемедицинских технологий осуществляются в целях:

1) **профилактики**, **сбора, анализа жалоб** пациента и данных **анамнеза**, **оценки эффективности лечебно-диагностических мероприятий**, медицинского **наблюдения** за состоянием здоровья пациента

2) **принятия решения о необходимости проведения очного приема** (осмотра, консультации)

Федеральный закон от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»

Коррекция ранее назначенного лечения

3. При проведении консультаций с применением телемедицинских технологий **лечащим врачом** может осуществляться коррекция ранее назначенного лечения при условии установления им диагноза и назначения лечения на очном приеме (осмотре, консультации)

Лечащим врачом в ряде случаев может быть фельдшер

Федеральный закон от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»

Дистанционное наблюдение

4. **Дистанционное наблюдение** за состоянием здоровья пациента назначается **лечащим врачом** **после очного приема** (осмотра, консультации). Дистанционное наблюдение осуществляется на основании данных о пациенте, зарегистрированных с применением **медицинских изделий**, предназначенных для мониторинга состояния организма человека, и (или) на основании данных, внесенных в единую государственную информационную систему в сфере здравоохранения, или государственную информационную систему в сфере здравоохранения субъекта Российской Федерации, или медицинскую информационную систему, или информационные системы, указанные в части 5 статьи 91 настоящего Федерального закона

Федеральный закон от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»

Персональные и медицинские данные, идентификация

6. В целях идентификации и аутентификации участников дистанционного взаимодействия при оказании медицинской помощи с применением телемедицинских технологий используется **единая система идентификации и аутентификации**

7. Документирование информации об оказании медицинской помощи пациенту с применением телемедицинских технологий, включая внесение сведений в его медицинскую документацию, осуществляется с использованием **усиленной квалифицированной электронной подписи медицинского работника**

Федеральный закон от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»

2.3. Порядок оказания медицинской помощи с применением телемедицинских технологий

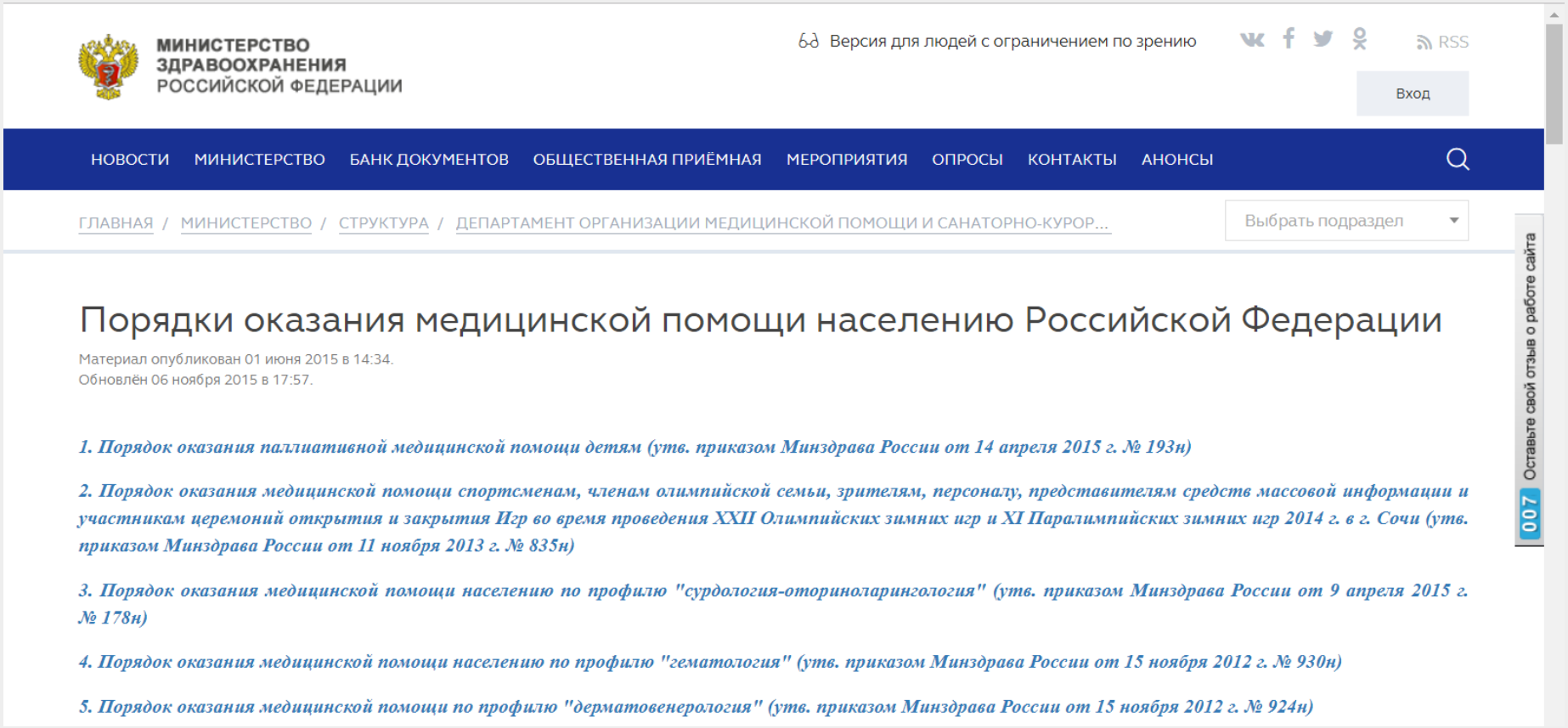
Порядки оказания медицинской помощи и стандарты медицинской помощи

- Федеральный закон от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» в статье 37 закрепляет, что «**медицинская помощь организуется и оказывается в соответствии с порядками оказания медицинской помощи**, обязательными для исполнения на территории Российской Федерации всеми медицинскими организациями, а также на основе стандартов медицинской помощи»
- Разработка государственных стандартов и порядков оказания медицинской помощи призваны выступить надлежащей гарантией доступности и качества медицинской помощи и соответствующих медицинских услуг (**как платных, так и бесплатных**) независимо от их места расположения и форм собственности

Порядки оказания медицинской помощи

- Порядки оказания медицинской помощи, направлены **на создание единообразия и упорядочивания оказания медицинских услуг** (как платных, так и бесплатных).
- В соответствии с пунктом 3 статьи 37 Федерального закона № 323-ФЗ порядок оказания медицинской помощи разрабатывается по:
  - **отдельным ее видам**
  - **профилям**
  - **заболеваниям или состояниям** (группам заболеваний или состояний)
- Порядок оказания медицинской помощи должен включать в себя:
  - **Правила организации** деятельности медицинской организации (ее подразделения, конкретного врача)
  - **Стандарт оснащения** медицинской организации
  - **Штатные нормативы** медицинской организации
  - **Этапы оказания** медицинской помощи
  - Иные положения

На 2018 год утверждено более 60 порядков



https://www.rosminzdrav.ru/ministry/61/4/stranitsa-857/poryadki-okazaniya-meditsinskoy-pomoschi-naseleniyu-rossiyskoy-federatsii

Порядки и стандарты при применении ТМ технологий

Статья 36.2. Особенности медицинской помощи, оказываемой с применением телемедицинских технологий

1. Медицинская помощь с применением телемедицинских технологий организуется и оказывается в **порядке**, установленном уполномоченным федеральным органом исполнительной власти, а также **в соответствии с порядками** оказания медицинской помощи и на основе **стандартов медицинской помощи**

Федеральный закон от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»

Приказ Минздрава России от 30.11.2017 №965н «Об утверждении порядка организации и оказания медицинской помощи с применением телемедицинских технологий» (Зарегистрировано в Минюсте России 09.01.2018 N 49577)

Основные положения

- Порядок регламентирует применение телемедицинских технологий
- Применяется для медицинскими организациями **всех форм собственности**
- Регулирует применение ТМ технологий:
  - при дистанционном взаимодействии **медицинских работников между собой**
  - при дистанционном взаимодействии **медицинских работников с пациентами** и (или) их законными представителями
  - при **дистанционном мониторинге** состояний здоровья

Для применения телемедицинских технологий в клинической практике

- Врачу **нет необходимости получать отдельный сертификат** – деятельность врача осуществляется в рамках действующей специальности
- Клинике **нет необходимости получать отдельную лицензию** – деятельность клиники осуществляется в рамках действующей лицензии по профилям медицинской организации

Формат дистанционного взаимодействия

- Аудиосвязь
- Видеосвязи
- Передачи электронных сообщений – текстовые, графические элементы и пр.
- Режим:
  - в режиме реального времени
  - в режиме отложенных консультаций

Ведение документации

- Необходимо использование **усиленной квалифицированной электронной подписи**
- По результатам применения ТМ технологий необходимо **внесение сведений в медицинскую документацию** (электронную историю болезни и пр.)
- **Все материалы**, полученные по результатам дистанционного взаимодействия **подлежат хранению**

Виды помощи где может быть применены ТМ технологии

- Первичной медико-санитарной помощи
- Специализированной, в том числе высокотехнологичной, медицинской помощи
- Скорой, в том числе скорой специализированной, медицинской помощи
- Паллиативной медицинской помощи

Все виды медицинской помощи!

Место оказания медицинской помощь с применением телемедицинских технологий

- В любых условиях:
  - вне медицинской организации
  - амбулаторно
  - в дневном стационаре
  - стационарно
- Условия оказания помощи определяются фактическим местонахождением пациента

Оплата за ТМ

а) **Бесплатно** – в рамках программы государственных гарантий бесплатного оказания гражданам Российской Федерации медицинской помощи за счет средств обязательного медицинского страхования и средств соответствующих бюджетов, а также в иных случаях, установленных законодательством Российской Федерации

б) **Платно** – на возмездной основе за счет личных средств граждан, средств юридических лиц и иных средств на основании договоров, в том числе договоров добровольного медицинского страхования

Ответственность

- **Ответственность за медицинское заключение** (протокол консилиума врачей) по результатам консультации или консилиума врачей с применением телемедицинских технологий, лежит **на консультанте** (врачах – участниках консилиума)
- **Ответственность за принятие решений** при оказании медицинской помощи с применением телемедицинских технологий лежит **на лечащем враче**, за исключением случаев, установленных нормативными актами

Требования к регистрации медицинских организаций и работников

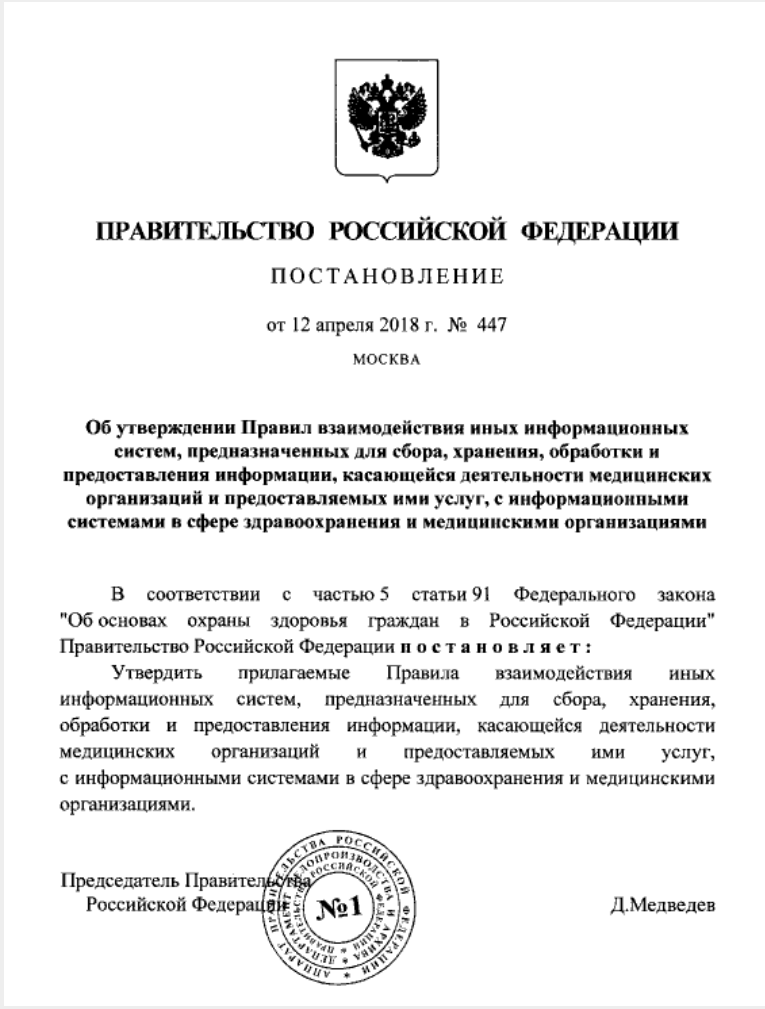
- Требуется предварительная **регистрация медицинских организаций** в Федеральном **реестре медицинских организаций** Единой государственной информационной системы в сфере здравоохранения (Единой системе)
- Требуется регистрация **медицинских работников** в Федеральном **регистре медицинских работников**

Медицинские изделия и программное обеспечение

- **Специальное программное обеспечение**, предназначенное для профилактики, диагностики, лечения и медицинской реабилитации заболеваний, мониторинга состояния организма человека **подлежит регистрации в качестве медицинских изделий**
- **Медицинские изделия**, предназначенные для использования при оказании медицинской помощи с применением телемедицинских технологий, подлежат регистрации в установленном порядке

Программные платформы для оказания ТМ

- Единая система (**ЕГИСЗ**)
- Государственная информационная системы в сфере здравоохранения **субъекта** Российской Федерации
- Медицинские информационные системы **медицинской организации**
- **Иные** информационные системы (все коммерческие информационные платформы)



ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 12 апреля 2018 г. № 447

МОСКВА

Об утверждении Правил взаимодействия иных информационных систем, предназначенных для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг, с информационными системами в сфере здравоохранения и медицинскими организациями

В соответствии с частью 5 статьи 91 Федерального закона "Об основах охраны здоровья граждан в Российской Федерации" Правительство Российской Федерации **п о с т а н о в л я е т :**

Утвердить прилагаемые Правила взаимодействия иных информационных систем, предназначенных для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг, с информационными системами в сфере здравоохранения и медицинскими организациями.

Председатель Правительства Российской Федерации Д.Медведев

http://publication.pravo.gov.ru/Document/View/0001201804160037?index=0&rangeSize=1

Порядок проведения консультаций (консилиумов врачей)

Лечащий врач устанавливает необходимость консультации

Лечащий врач проводит предварительное обследование, пересылает данные и/или передает доступ к данных

Консультант (врачи участники консилиума)

Проводит консультацию

Медицинское заключение

Электронная подпись

Отправка заключения лечащему врачу

Порядок взаимодействии медицинских работников с пациентами и (или) их законными представителями

Дистанционное наблюдение за состоянием здоровья пациента

- **После очного приема** (осмотра, консультации) и установления диагноза заболевания
- Дистанционное наблюдение **осуществляет лечащий врач**
- **Применяются**:
  - Ручной ввод данных о состоянии здоровья пациента
  - Программное обеспечение
  - Медицинские приборы
- **Врач**
  - Осуществляет контроль за показателями
  - Регистрирует данные в электронной медицинской карте пациента
  - Корректирует назначения
- **Пациент (представитель)**
  - Вводит данные, использует приборы
  - Следит за работоспособностью приборов
  - Выполняет назначения

2.4. Дистанционное наблюдение за состоянием здоровья

Эволюция медицинского оборудования

Фото автора

Тенденции и возможности

- Миниатюризация
- Использование стандартных IT решений
- Возможность подключения к сети
- Передача данных в формализованном цифровом виде (DICOM, HL7)
- Облачное хранилище данных
- Многопользовательский многоуровневый удаленный доступ к данным

Бытовые приборы, одежда

Медицинские приборы

Интернет медицинских вещей

Фото автора
http://ettagroup.ru/

Интернет медицинских вещей

Интернет медицинских вещей (англ. Internet of Medical Things, IoMT) – это концепция сети, объединяющей «подключённые устройства» и приборы, которые отслеживают состояние организма человека и окружающей его среды, включая приборы, способные интерактивно влиять на профилактический, лечебный и реабилитационный процессы

Фото автора

Облачные технологии – место сбора данных

От стационарной лаборатории – к персональному мониторингу физиологических функций

Позволяет перейти от дискретного обследования к непрерывному мониторингу

Технология интернета медицинских вещей

Клинические аспекты применения

- **Диагностические**: тонометр, анализатор мочи, УЗ-аппарат, глюкометр, термометр, урофлоуметр и др.
- **Профилактические:** для ведения здорового образа жизни (wellness) – фитнес-трекер, весы и пр.
- **Лечебные:** инсулиновая помпа, «умная» таблетница, которая контролирует прием препаратов и др.
- **Реабилитационные**

Диагностические приборы

- **Скрининг и ранняя диагностика**
- **Наблюдение** — мониторинг физиологических функций организма

Мониторинг

Фиксированные: Метеостанция

Портативные: Портативный мочевой анализатор

Носимые: Фитнес-трекер

Имплантируемые: «Умная» татуировка

Фото автора
http://ettagroup.ru/
Фото автора
https://evercare.ru/flexible-gold-skin

Приборы по целевым группам пользователей

- **Медицинские** — основные пользователи - медицинские работники (врачи, фельдшеры, медицинские сестры и др.).
- **Домашние приборы** — основные пользователи этих приборов – пациенты и люди, желающие вести здоровый образ жизни.
- **Профессиональные** — спортсмены, сотрудники службы охраны, военные, пожарные, работники удаленных буровых станций, водители

Фото автора

Регистрация медицинских изделий

- Приборы класса «интернет медицинских вещей» могут использоваться для принятия клинических решений
- В связи с этим попадают под статус «медицинских изделий»
- Подлежат медицинской регистрации

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ ЗДРАВООХРАНЕНИЯ

http://www.roszdravnadzor.ru/

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ ЗДРАВООХРАНЕНИЯ (РОСЗДРАВНАДЗОР)

РЕГИСТРАЦИОННОЕ УДОСТОВЕРЕНИЕ НА МЕДИЦИНСКОЕ ИЗДЕЛИЕ

от 30 мая 2016 года № РЗН 2016/4153

На медицинское изделие
Портативный анализатор мочи "ЭТТА АМП-01" на тест-полосках по ТУ 9443-001-17140544-2015

Настоящее регистрационное удостоверение выдано
Общество с ограниченной ответственностью "ЭТТА" (ООО "ЭТТА"), Россия, 107031, Москва, ул. Рождественка, д. 5/7, к. 2, оф. V, ком. 7

Производитель
Общество с ограниченной ответственностью "ЭТТА" (ООО "ЭТТА"), Россия, 107031, Москва, ул. Рождественка, д. 5/7, к. 2, оф. V, ком. 7

Место производства медицинского изделия
111020, Москва, ул. Боровая, д. 7, стр. 7

Номер регистрационного досье **№ РД-8725/47242 от 01.10.2015**

Вид медицинского изделия **113990**

Класс потенциального риска применения медицинского изделия **2а**

Код Общероссийского классификатора продукции для медицинского изделия **94 4310**

Настоящее регистрационное удостоверение имеет приложение на 1 листе

приказом Росздравнадзора от 30 мая 2016 года №4399
допущено к обращению на территории Российской Федерации.

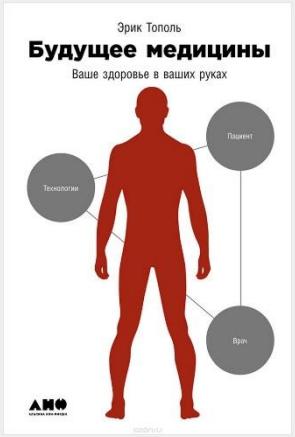
Руководитель Федеральной службы по надзору в сфере здравоохранения **М.А. Мурашко**

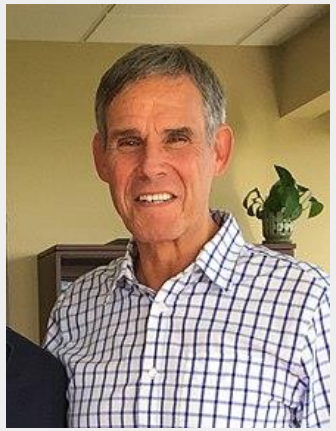
0014084

http://ettagroup.ru/

Географическая информационная система (ГИС) человека по Эрику Тополю

- **Геном**
- **Транскриптом**
- **Протеом**
- **Метаболом**
- **Микробиом**
- **Эпигеном**
- **Экспосом**
- Данные полученные с помощью разнообразных **методов визуализации**
- Информация, полученная с **биосенсоров**
- **Социальные графы**

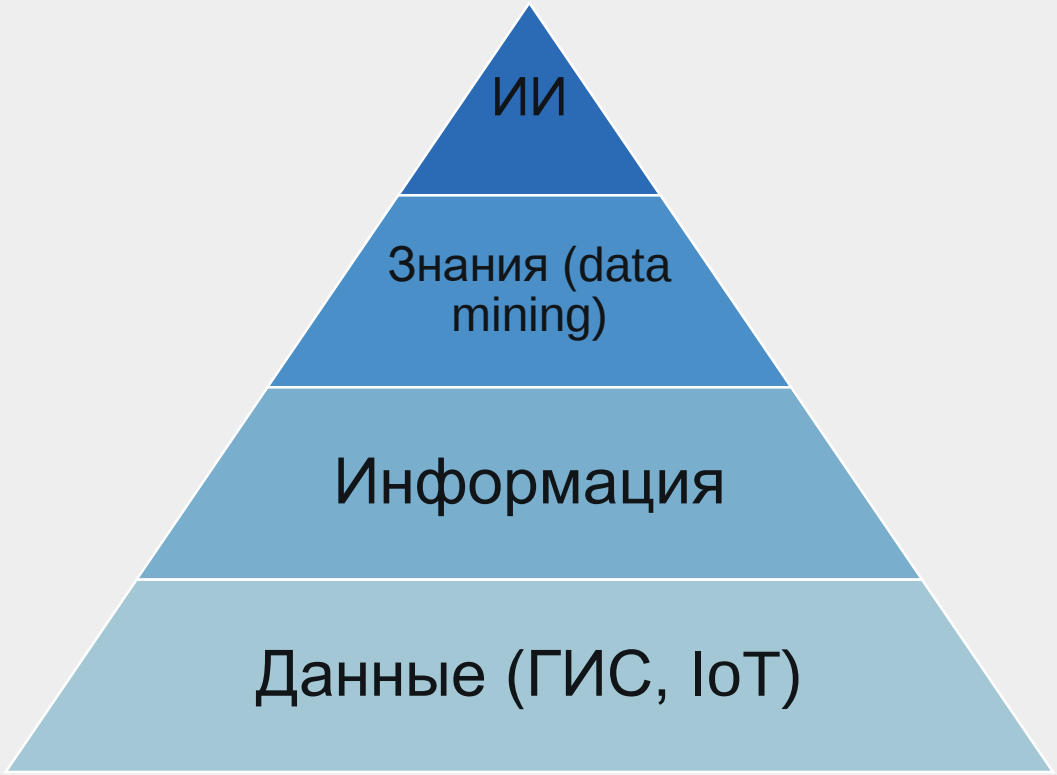


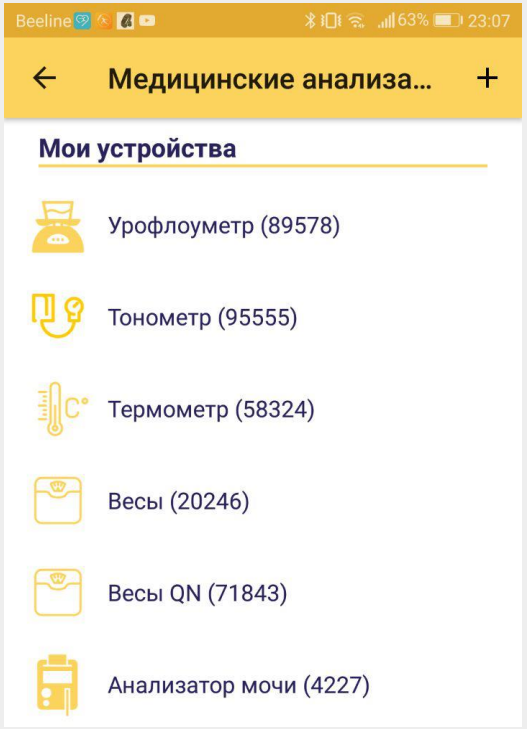


Будущее медицины. Ваше здоровье в ваших руках

https://www.ozon.ru/context/detail/id/137789447/
https://en.wikipedia.org/wiki/Eric_Topol

Пирамида данных, на которых базируется искусственный интеллект (ИИ) в медицине





https://nethealth.ru/

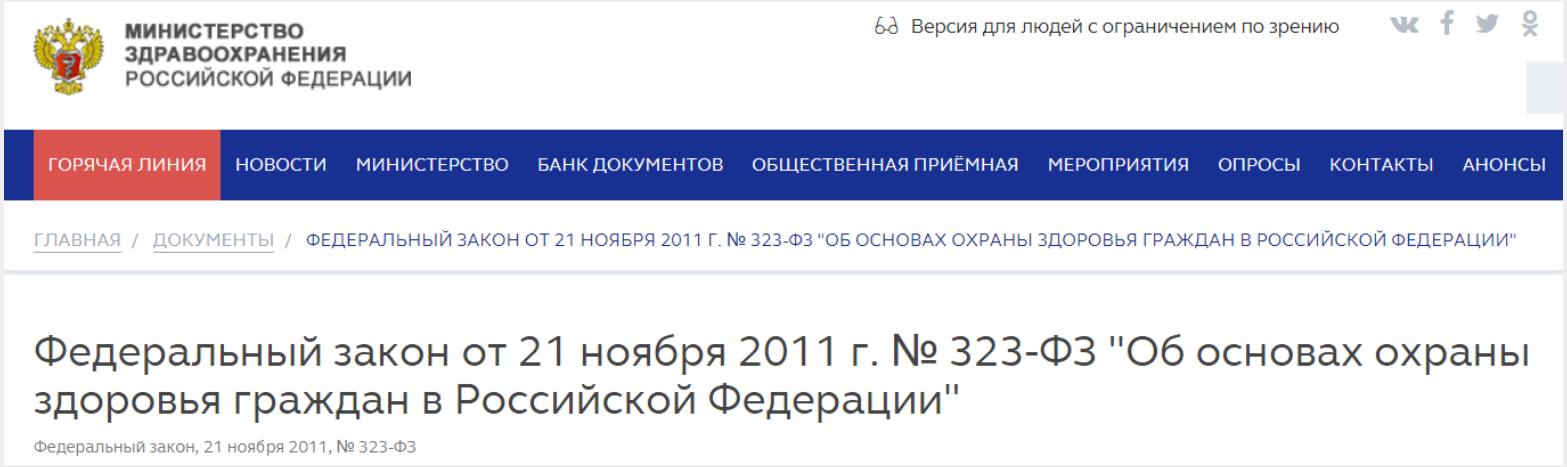
Большие данные, получаемые с приборов класса «интернет медицинских вещей»

2.5. Телемедицинский домашний стационар

Медицинская помощь может оказываться в следующих условиях

Статья 32. Медицинская помощь

1. **вне медицинской организации** (по месту вызова бригады скорой, в том числе скорой специализированной, медицинской помощи, а также в транспортном средстве при медицинской эвакуации)
2. **амбулаторно** (в условиях, не предусматривающих круглосуточного медицинского наблюдения и лечения), **в том числе на дому** при вызове медицинского работника
3. **в дневном стационаре** (в условиях, предусматривающих медицинское наблюдение и лечение в дневное время, но не требующих круглосуточного медицинского наблюдения и лечения)
4. **стационарно** (в условиях, обеспечивающих круглосуточное медицинское наблюдение и лечение)



https://www.rosminzdrav.ru/

Положение о стационаре на дому

«Погружено» в Приказ Министерства здравоохранения и социального развития РФ от 15 мая 2012 г. N 543н «Об утверждении Положения об организации оказания первичной медико-санитарной помощи взрослому населению»

Лицензирование

- Стационар на дому создается при ЛПУ
- Работы и услуги, осуществляемые в стационаре на дому, подлежат лицензированию в составе ЛПУ
- **Достаточно иметь лицензию на амбулаторную помощь**

3. Медицинская помощь может оказываться в следующих условиях:

1) вне медицинской организации (по месту вызова бригады скорой, в том числе скорой специализированной, медицинской помощи, а также в транспортном средстве при медицинской эвакуации);

2) амбулаторно (в условиях, не предусматривающих круглосуточного медицинского наблюдения и лечения), в том числе на дому при вызове медицинского работника;

3) в дневном стационаре (в условиях, предусматривающих медицинское наблюдение и лечение в дневное время, но не требующих круглосуточного медицинского наблюдения и лечения);

4) стационарно (в условиях, обеспечивающих круглосуточное медицинское наблюдение и лечение).

https://www.rosminzdrav.ru/

Федеральный закон от 21.11.2011 N 323-ФЗ (ред. от 03.08.2018) «Об основах охраны здоровья граждан в Российской Федерации»

Преимущества стационара на дому

- **Снижение стоимости** лечения
- Уменьшение риска **госпитальной инфекции**
- Пациент находится в более **благоприятном психоэмоциональном состоянии** за счет привычной ему обстановки и окружения
- **Ответственность за близкого человека**
  - Воспитывает терпимость, взаимопонимание, дает возможность проявить заботу о близком

Новые возможности

- **Диагностические исследования** в домашних условиях
- **Коммуникации** между врачом, медицинским персоналом, осуществляющим динамическое наблюдение, и пациентом и/или его представителями, включая ухаживающий за ним персонал

Это позволяет говорить об **удаленном мониторинге** состояния пациента

Диагностика по месту оказания медицинской помощи – «point of care» (POC)

- **Компактность**
- **Мобильность**
- **Невысокая стоимость** (относительно стационарных приборов)
- **Простота** использования
- Практически **нет ограничений по количеству исследований** в течение периода наблюдения

Фото автора

Мобильный мочевой анализатор, УЗИ, урофлоуметр – из набора приборов (укладки) для урологического домашнего стационара

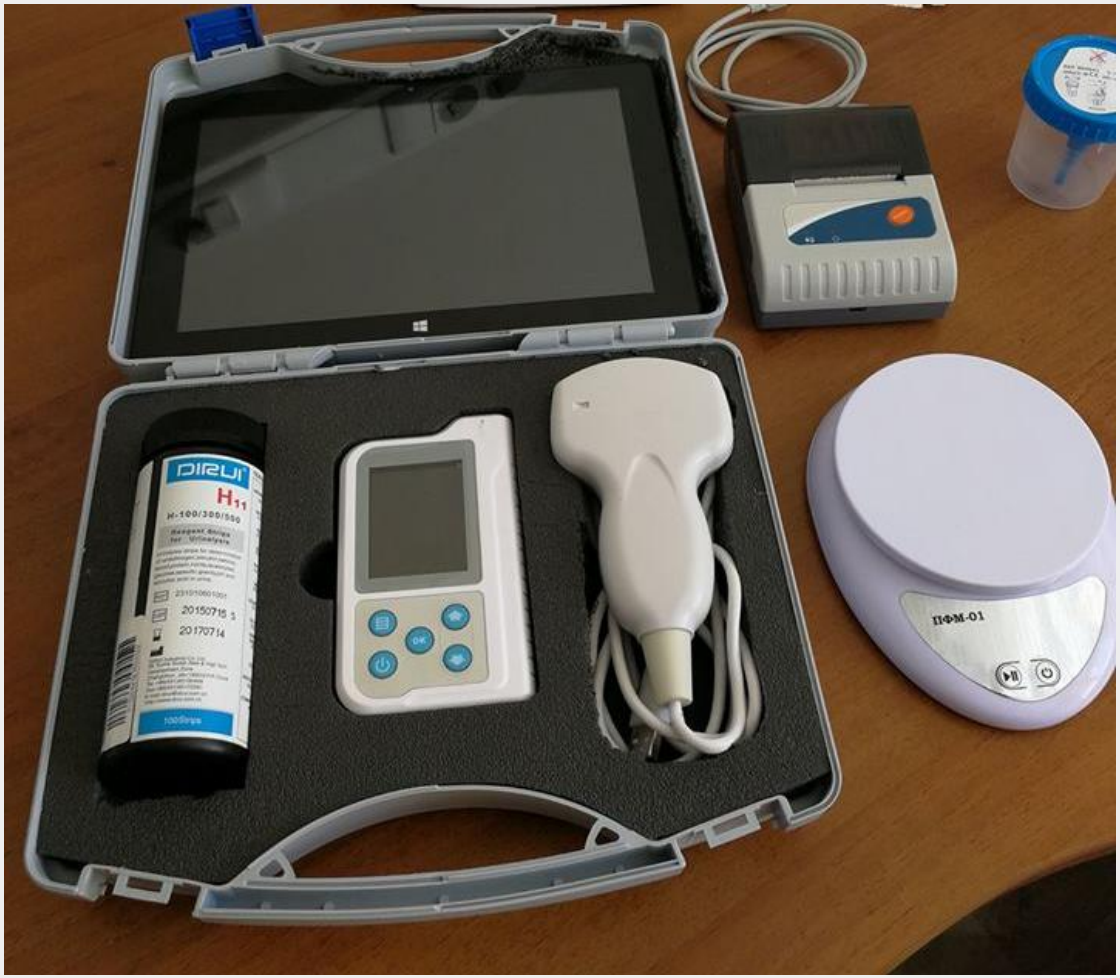


Фото автора

Стандартизированные наборы (укладки)

- Диагностическое оборудование, используемое для мониторинга лечебного процесса, рационально объединять в **стандартизированные наборы (укладки)**
- Могут использовать **у пациентов со схожими диагнозами** или группами **по врачебным специальностям**
- Такой подход позволяет:
  - Реализовать **модель аренды** оборудования на период организации дневного стационара
  - Делает более **удобным процесс подключения** этого оборудования к информационной системе
  - **Стандартизирует** назначения врача
  - Позволяет обеспечить **преемственность** лечебно-диагностического процесса

УРОЛОГИЯ

А. Общая укладка

- Портативный мочевой анализатор
- Весы напольные с биоимпедансометрией
- Термометр инфракрасный ушной
- Программное обеспечение

Б. Дополнительные опции для конкретных нозологических единиц

1) Доброкачественная гиперплазия предстательной железы (ДГПЖ, аденома простаты),

- Портативный урофлоуметр
- Трекер для контроля ночных вставаний (контроль ноктурии)

2) Мочекаменная болезнь

- Умная кружка с контролем количества выпитой жидкости

3) Нейрогенные нарушения функции органов малого таза

- Портативный УЗИ с функций определения объема остаточной мочи
- Портативный урофлоуметр
- Система тренировки мышц тазового дна с биологической обратной связью
- Ультразвуковая система мониторинга уровня наполнения мочевого пузыря

4) Андрогенный дефицит (врожденный и приобретенный)

- Портативный прибор для мониторинга уровня тестостерона
- Электронная линейка (пояс) для измерения окружности талии
- Браслет для постоянного ношения с функциями оценки дневной физической активности, мониторинга частоты пульсы, пульсовой волны, одноканального ЭКГ

5) Мужское бесплодие

- Портативный спермоанализатор

Каналы коммуникации в условиях домашнего стационара

Цель – возможность осуществления **коммуникации** врача, медицинского работника с наблюдаемым пациентом и его представителями

Задачи:

- Контроль **состояния пациента**
- Контроль **выполнения процедур**
- Улучшает **аттрактивность** к лечебному процессу, приближая его к условиям, аналогичным обычному стационару, в котором врач осуществляет регулярные (ежедневные) очные обходы своих пациентов

Видеоконференц связь

- **Качество** канала и оборудования **должно быть высоким** – это критично для стационара на дому
- Предпочтительно использовать **специализированное оборудование**
- **Частота и длительность** коммуникаций зависит от тяжести состоянии пациента:
  - Решение принимает лечащий врач
  - Эти показатели должны быть не меньше, чем такие же, при пребывании аналогичного пациента в госпитале
  - Рекомендуем это делать не реже 1 раза в сутки и длительностью не менее 15 минут за весь период наблюдения за пациентом в условиях домашнего стационара

Отсроченный канал связи

- **Дополнение** к ВКС
- С помощью **текстовых сообщений**
- **Быстрое решение текущих вопросов**, которые могут возникать в ходе мониторинга за состоянием пациента
- **Все направления**: лечащий врач, медицинский персонал, пациент, его близкие и ухаживающий персонал

Резервный канал связи

- **Телефонная связь**
- Используется в случае возникновения сложностей в использовании ВКС, тестовых сообщений (плохая связь, отсутствие интернета)
- Все заинтересованные лица должны иметь функционирующие телефоны (стационарные или мобильные) и актуальные номера

Информационная мониторинговая система домашнего стационара

- **Дистанционный мониторинг** состояния здоровья пациента – получение информации с подключенных приборов
- Ведения **плана лечения** пациента и контроля его выполнения
- Ведения электронной **истории болезни** (ИБ)
- **Экономико-статистический учет** медицинских услуг
- **Договор** об условиях оказания услуг, информированное согласие пациента на обработку персональных данных и др.