Информационная безопасность в ОУ

БЛОК «ИКТ», ЛЕКЦИЯ 2

Понятие информационной безопасности

В Доктрине информационной безопасности Российской Федерации: Информационная безопасность - состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

В Законе РФ "Об участии в международном информационном обмене" : Информационная безопасность - состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

ГОСТ "Защита информации. Основные термины и определения" (ГОСТ Р 50922-2006): Информационная безопасность - состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

ГОСТ "Защита информации. Основные термины и определения" (ГОСТ Р 50922-2006)

Конфиденциальность – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.

Целостность – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;

Доступность – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

В контексте обработки информации в образовательной организации

Информационная безопасность - защищенность информации и информационной образовательной среды от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и информационной образовательной среды.

Защита информации

Комплекс правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

Основные понятия:

объект защиты информации – это информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации;

защищаемая информация – это информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;

защищаемая информационная система – это информационная система, предназначенная для обработки защищаемой информации с требуемым уровнем ее защищенности.

Основные понятия:

техника защиты информации – это средства защиты информации, в том числе средства физической защиты информации, криптографические средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

средство защиты информации - это техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

средство физической защиты информации – это средство защиты информации, предназначенное или используемое для обеспечения физической защиты объекта защиты информации. **Угрозы информационной безопасности** – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Источник угрозы безопасности информации – это субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

Угроза является следствием наличия уязвимых мест или уязвимостей в информационной системе

Классификации угроз:

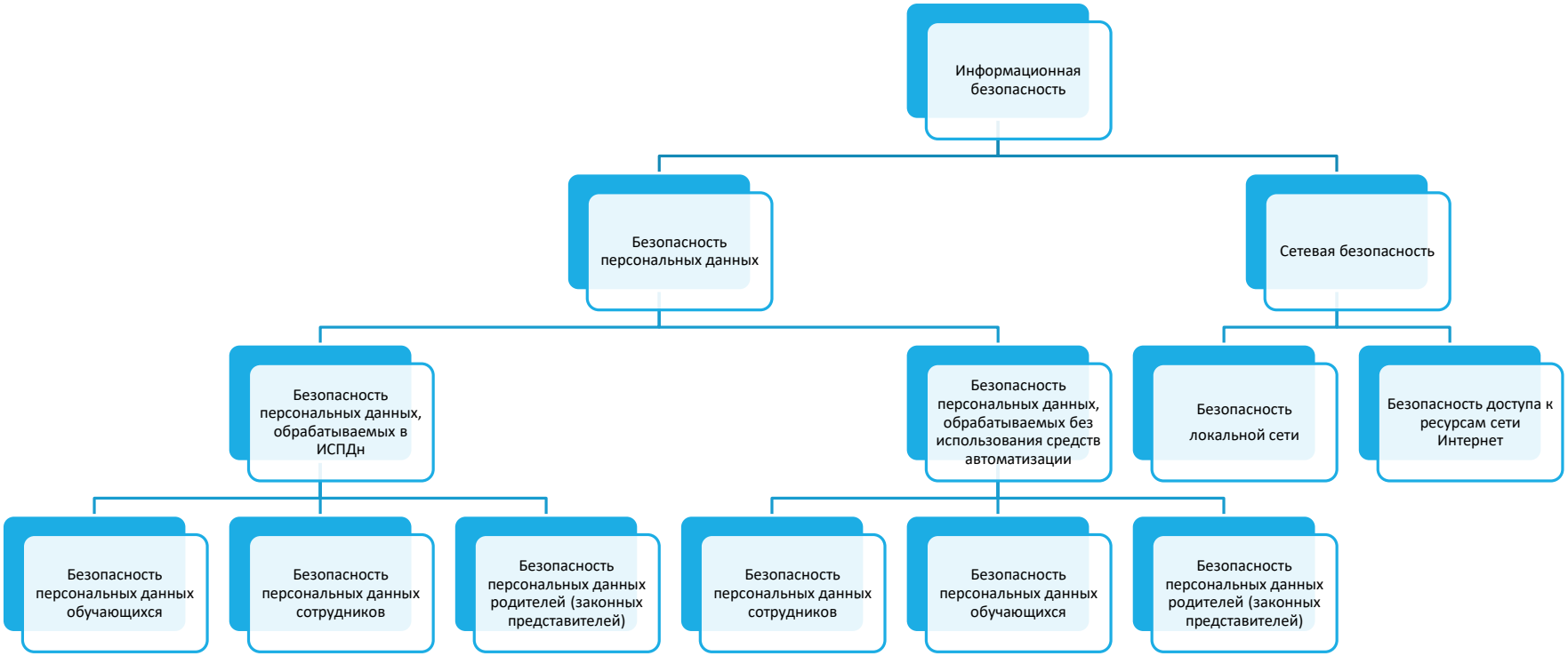
по свойствам информации (доступность, целостность, конфиденциальность), против которых угрозы направлены в первую очередь;

по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);

по способу осуществления (случайные/преднамеренные, действия природного/техногенного характера);

по расположению источника угроз (внутри/вне рассматриваемой ИС).

Основные направления обеспечения информационной безопасности в ОО



Уровни обеспечения информационной безопасности

законодательный – законы, нормативные акты и прочие документы РФ;

административный – комплекс мер, предпринимаемых руководством образовательной организации;

процедурный уровень – меры безопасности, реализуемые людьми;

программно-технический уровень – непосредственно средства защиты информации.

Принципы построения системы информационной безопасности

- Принцип непрерывности совершенствования и развития системы информационной безопасности.

Обеспечение информационной безопасности не может быть одноразовым актом.

- Принцип комплексного использования всего арсенала имеющихся средств защиты.

Условия обеспечения информационной безопасности:

законность,

достаточность,

соблюдение баланса интересов личности и образовательной организации,

высокий профессионализм представителей службы информационной безопасности,

подготовка пользователей и соблюдение ими всех установленных правил сохранения конфиденциальности,

взаимная ответственность педагогов и руководства.

Требования к системе обеспечения информационной безопасности

Централизованность системы обеспечения информационной безопасности.

Запланированность мероприятий по обеспечению информационной безопасности.

Целенаправленность системы обеспечения информационной безопасности.

Активность системы.

Надежность и универсальность.

Нестандартность и разнообразность.

Открытость для изменения и дополнения.

Экономическая эфективность.

Рекомендации по созданию системы информационной безопасности:

средства защиты должны быть просты для технического обслуживания и “прозрачны” для пользователей;

каждый пользователь должен иметь минимальный набор привилегий, необходимых для работы;

независимость системы защиты от субъектов защиты;

учет враждебности окружения (предполагаем, что пользователи имеют наихудшие намерения, будут совершать серьезные ошибки и искать пути обхода механизмов защиты);

отсутствие излишней информации.

Нормативно-правовая база федерального уровня

Федеральный закон «Об информации, информационных технологиях и защите информации» № 149-ФЗ от 27.07.2006 г.

Федеральный закон «О персональных данных» № 152-ФЗ от 27.07.2006 г.

Федеральный закон «О средствах массовой информации» № 2124-1 – РФ от 27.12.1991 г.

Федерального закона «О рекламе» № 38-ФЗ от 13.03.2006 г.

Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

Письмо Роспотребнадзора от 17.09.2008 № 01/10237-8-32 «О мерах, направленных на нераспространение информации, наносящей вред здоровью, нравственному и духовному развитию детей и подростков».

Постановление Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» № 687 от 15.09.2008 г.

Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» № 1119 от 01.11.2012 г.

Постановление правительства РФ «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» № 211 от 21 марта 2012 г.

Нормативно-правовая база федерального уровня

- Приказ ФСТЭК России “Об утверждении состава и содержания организационных и техническим мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных” №21 от 18.02.2013 г.
- Приказ ФСТЭК России “Об утверждении Требований к защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах” №17 от 11.02.2013 г.
- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные Приказом Гостехкомиссии России №282 от 30.08.2002 г.
- Письмо Роспотребнадзора от 17.09.2008 № 01/10237-8-32 «О мерах, направленных на нераспространение информации, наносящей вред здоровью, нравственному и духовному развитию детей и подростков».
- Письмо Министерства образования и науки Российской Федерации «Об обеспечении защиты персональных данных» №17-110 от 29.07.2009.

ФЗ № 149 “Федеральный закон об информации…”

Статья 3. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации.

*1) **свобода** поиска, **получения**, передачи, производства и распространения **информации** любым законным способом;*

*2) **установление ограничений** доступа к информации **только федеральными законами**;*

*3) открытость информации **о деятельности государственных органов и органов местного самоуправления** и **свободный доступ к** такой **информации**, кроме случаев, установленных федеральными законами…*

ФЗ № 149 “Федеральный закон об информации…”

Статья 15.1. Единый реестр доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию,распространение которой в Российской Федерации запрещено (введена Федеральным законом от 28.07.2012 N **139-ФЗ**)

***п1. В целях ограничения доступа к сайтам в сети "Интернет"**, содержащим информацию, распространение которой в Российской Федерации запрещено, **создается единая** автоматизированная **информационная система** "Единый реестр доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено" (**далее - реестр**).*

eais.rkn.gov.ru

ФЗ № 436 “О защите детей от информации, причиняющей вред их здоровью и развитию”

Статья 5. Виды информации, причиняющей вред здоровью и (или) развитию детей

п2. К информации, **запрещенной** для распространения среди детей, относится информация:

*1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к **причинению вреда своему здоровью, самоубийству**;*

*2) способная вызвать у детей желание **употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством**;*

*3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять **насильственные действия по отношению к людям или животным**, за исключением случаев, предусмотренных настоящим Федеральным законом;*

*4) **отрицающая семейные ценности**, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи;*

*5) **оправдывающая противоправное поведение**;*

*6) **содержащая нецензурную брань**;*

*7) содержащая **информацию порнографического характера**;*

*8) **о несовершеннолетнем, пострадавшем в результате противоправных действий**...*

ФЗ № 436 “О защите детей от информации, причиняющей вред их здоровью и развитию”

Статья 5. Виды информации, причиняющей вред здоровью и (или) развитию детей

п3. К информации, распространение которой **среди детей определенных возрастных категорий ограничено**, относится информация:

*1) представляемая в виде **изображения или описания жестокости**, физического и (или) психического **насилия**, **преступления** или иного антиобщественного действия;*

*2) **вызывающая** у детей **страх, ужас или панику**, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;*

*3) представляемая в виде **изображения или описания половых отношений** между мужчиной и женщиной;*

*4) содержащая **бранные слова и выражения, не относящиеся к нецензурной брани**.*

Статья 6. Осуществление классификации информационной продукции

п3. Классификация…

*2) информационная продукция для детей, достигших возраста **шести лет**;*

*3) информационная продукция для детей, достигших возраста **двенадцати лет**;*

*4) информационная продукция для детей, достигших возраста **шестнадцати лет**;*

ФЗ № 436 “О защите детей от информации, причиняющей вред их здоровью и развитию”

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

*1) доступ детей к информации - **возможность получения и использования детьми свободно распространяемой информации**;*

Статья 11 (14). Общие требования к обороту информационной продукции

***п2. Оборот информационной продукции**, содержащей информацию, запрещенную для распространения среди детей в соответствии с частью 2 статьи 5 настоящего Федерального закона, **в местах, доступных для детей, не допускается без применения административных и организационных мер, технических и программно-аппаратных средств защиты** детей от указанной информации.*

***п3. Требования к** административным и организационным мерам, техническим и программно-аппаратным **средствам защиты** детей от информации, причиняющей вред их здоровью и (или) развитию, **устанавливаются уполномоченным** Правительством Российской Федерации **федеральным органом исполнительной власти**.*

Минобрнауки (для школ)

2006 г. - **рассылка ПО СКФ** (Netpolice) в рамках проекта “1 помощь”.

2011 г. - Правила **подключения ОУ** к системе контент-фильтрации (Минобрнауки N АФ-12/07внб 2011) - *на базе опять же ПО СКФ (Netpolice) через регистрацию **на сайте skf.edu.ru**.*

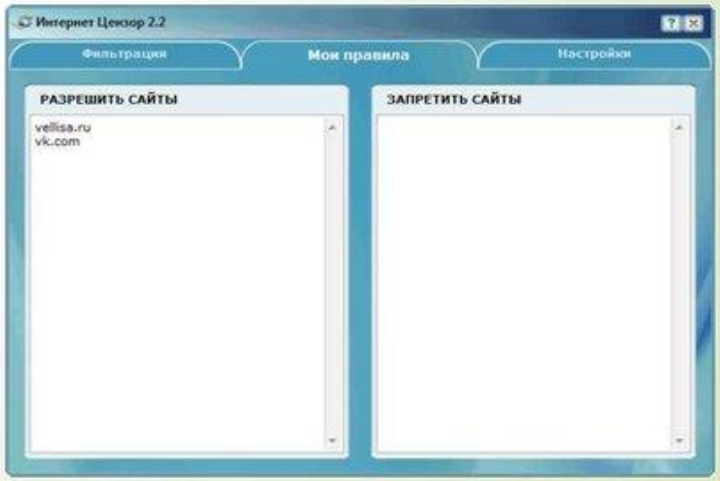
2014 г. - Методические рекомендации по ограничению в ОУ доступа обучающихся к видам информации, распространяемой посредством сети «Интернет» (Минсвязи, Минобрнауки).

Минобрнауки (для детских садов)

Интернет Цензор

Официальный сайт
https://vellisa.ru/internet-tsenzor

Интернет Цензор — бесплатная программа для осуществления родительского контроля. Программа предназначена для эффективной блокировки сайтов, которые могут представлять опасность для ребенка, когда он использует Интернет.



Методические рекомендации ... (Минкомсвязи, Минобрнауки, 2014г)

3.4. Ответственность.

В соответствии со статьей 6.17 Кодекса Российской Федерации об административных правонарушениях от 30 декабря 2001 г. No 195-ФЗ **руководитель образовательной организации несет ответственность за нарушение законодательства Российской Федерации** о защите детей
от информации, причиняющей вред их здоровью и (или) развитию.

Федеральный **закон** No 436-ФЗ **не определяет ответственность поставщиков СКФ** за ненадлежащее оказание услуги по ограничению доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования (далее - услуга).

В связи с этим **рекомендуется в договоре**, заключаемом с поставщиком СКФ, **указывать ответственность и обязательства поставщика СКФ** в виде компенсации понесенного ущерба за ненадлежащее оказание услуги.

Методические рекомендации … (Минкомсвязи, Минобрнауки, 2014г)

В настоящем документе дается краткий обзор текущей ситуации в рамках поставленной задачи, проводится анализ существующей СКФ с соответствующими рекомендациями, и приводится вариант модернизации СКФ с учетом этих рекомендаций.

Главные рекомендации:

1. ***создание реестра НСОР (Не Совместимых с Образованием Ресурсов)***
2. ***перенести ответственность по организации оказания услуг контентной фильтрации на провайдеров сети интернет***

Документ в феврале **2014** года **прошёл экспертную оценку и был одобрен в Совете Федерации**, в апреле 2014 был одобрен на подкомиссии по использованию информационных технологий при предоставлении государственных и муниципальных услуг Правительственной комиссии по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности….

Паритет между необходимым и возможным

1. Есть **требование** свободного **доступа** к незапрещенной информации
2. Есть **требование ограничения** доступа к запрещенной информации
3. Есть **ответственность** руководителя ОУ
4. Есть **реестр запрещенных сайтов Роскомнадзора, Минюста**
5. Есть **список категорий для запрета** доступа детей
6. Есть правила подключения к СКФ
7. Есть реестр НСОР

Но

1. **Сайт** рекомендуемой СКФ (**skf.edu.ru**) **не функционирует**.

Ответственность поставщиков СКФ отсутствует, но есть ответственность административная оператора связи -КоАП РФ, Статья 13.34

Неисполнение оператором связи, оказывающим услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", **обязанности по ограничению** или возобновлению доступа к **информации**, доступ к которой должен быть ограничен или возобновлен на основании сведений, полученных от федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере связи, информационных технологий и массовых коммуникаций.

(введена Федеральным законом от 22.02.2017 N 18-ФЗ)

Как выглядят технические требования по подключениям к базам Контент-фильтра

– БД «Единый Реестр запрещенных доменных имен, указателей страниц сайтов Роскомнадзора РФ». Доступ к БД предоставляется в автоматическом режиме круглосуточно исключительно с использованием квалифицированной электронной подписи и лицензии оператора связи.

– БД сайтов Министерства Юстиции РФ. Автоматическое обновление через RSS-канал сайта Министерства Юстиции РФ.

– Реестр НСОР (Реестр Не Совместимых с Образованием Ресурсов)

– База данных Министерства Образования и Науки РФ. Система фильтрации прошла тестирование по интеграции Реестром НСОР и получает обновленные списки фильтрации.

Единая мультисервисная телекоммуникационная сеть (ЕМТС)

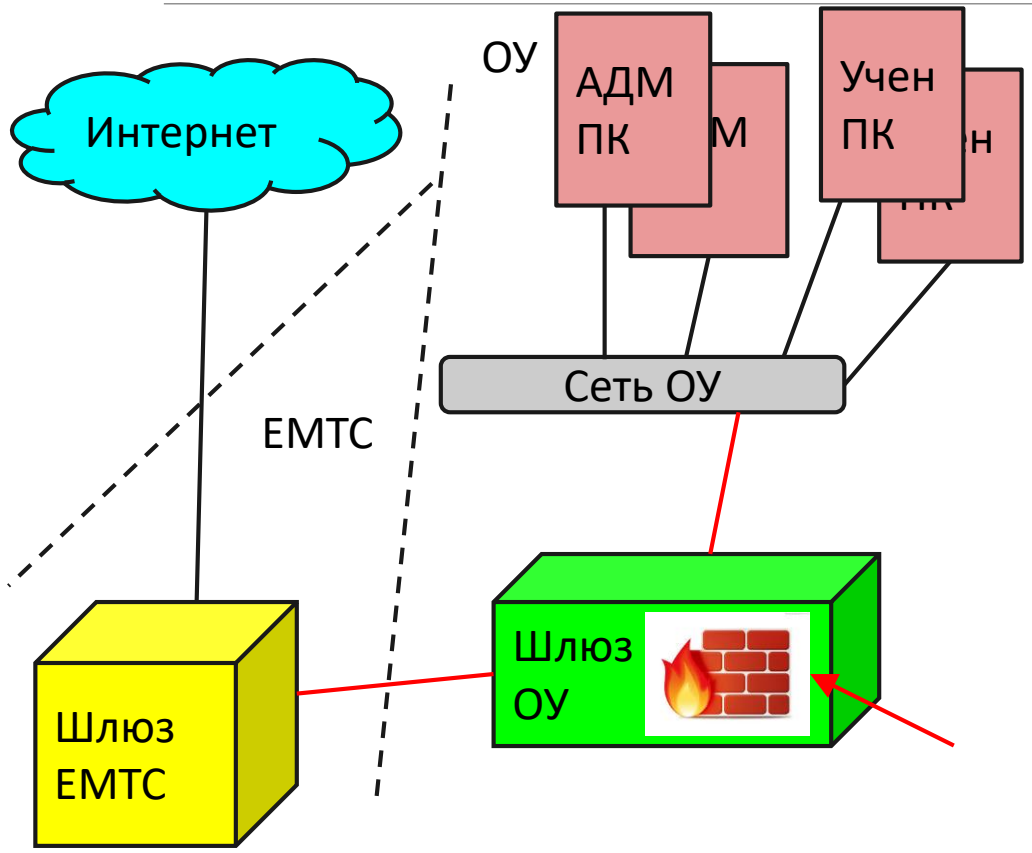
В соответствии с распоряжением Администрации Санкт-Петербурга № 227-ра от 19.02.2002 «О создании Единой мультисервисной телекоммуникационной сети исполнительных органов государственной власти Санкт-Петербурга» в Санкт-Петербурге с 2002 года успешно развивается и функционирует Единая мультисервисная телекоммуникационная сеть исполнительных органов государственной власти (далее – ЕМТС).

В настоящий момент к ЕМТС подключено более 2000 исполнительных органов государственной власти, подведомственных учреждений и городских объектов.

Что может ЕМТС?

- организовать скоординированное, централизованное ведение и использование баз данных общегородских автоматизированных информационных систем;
- обеспечить соблюдение требований информационной безопасности;
- объединить городские службы и организации в единую информационную систему для их оперативного взаимодействия на основе современных информационных технологий, как в повседневной деятельности, так и при возникновении экстремальных ситуаций;
- объединить исполнительные органы государственной власти и подведомственные им учреждения в единую телефонную сеть, что позволило снизить их зависимость от услуг сторонних операторов связи, а также сократить расходы на оплату услуг, арендуемых линий и каналов связи;
- организовать широкополосные высокоскоростные каналы доступа к информационно-коммуникационной сети «Интернет» для образовательных учреждений города.

До Интернет еще надо добраться...



Сервисы интернет = (TCP\IP)
= адреса + протоколы (порты)
№ Портов:
53 - DNS
80 - HTTP
443 - HTTPS
Межсетевой экран (firewall, брандмауэр)

Словарь

DNS (англ. *Domain Name System* — система доменных имён) — компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты, обслуживающих узлах для протоколов в домене (SRV-запись).

HTTP (англ. *HyperText Transfer Protocol* — «протокол передачи гипертекста») — протокол прикладного уровня передачи данных (изначально — в виде гипертекстовых документов в формате «HTML», в настоящий момент используется для передачи произвольных данных). Основой HTTP является технология «клиент-сервер», то есть предполагается существование: Потребителей (клиентов), которые инициируют соединение и посылают запрос; Поставщиков (серверов), которые ожидают соединения для получения запроса, производят необходимые действия и возвращают обратно сообщение с результатом.

HTTPS не является отдельным протоколом. Это обычный HTTP, работающий через шифрованные транспортные механизмы SSL и TLS. Он обеспечивает защиту от атак, основанных на прослушивании сетевого соединения, при условии, что будут использоваться шифрующие средства и *сертификат сервера проверен и ему доверяют*.

Что фильтруем?

ip-адрес 77.88.8.7

domain rcokoit.ru (umr.rcokoit.ru)

url http: // **yandex.ru** / pogoda / saint-petersburg

content содержимое страницы

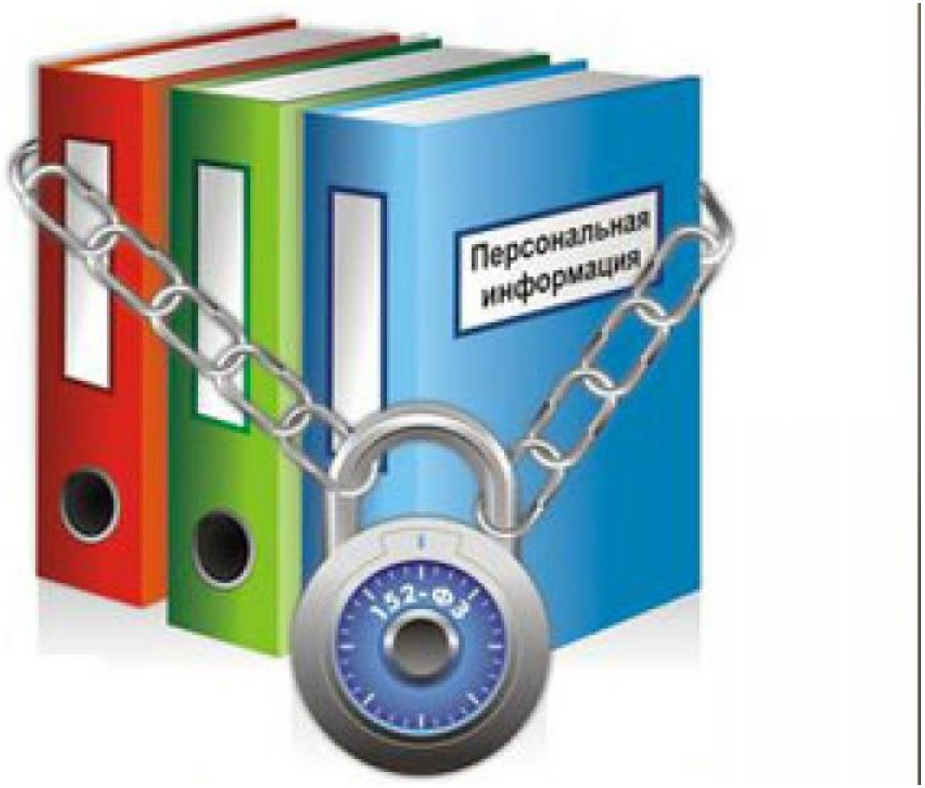
Подводим итоги

Из разговоров с прокуратурой:

1. **Фильтруем все ПК**, к которым у детей **может** быть доступ - компьютерные классы и ПК всех педагогов
2. Работаем по **белым спискам** сайтов
3. Имеем в ОУ и знакомим пользователей с **локальными актами** по использованию сети “Интернет” с “**регламентом добавления сайтов в белый список**”.

ПК в административных кабинетах фильтровать достаточно по черным спискам (см. ресурс antizapret.info)

Защита персональных данных



Основные понятия, связанные с обеспечением безопасности информации и персональных данных

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Содержание отдельных статей ФЗ “О персональных данных”
№ 152 – ФЗ от 27.07.2006 г.

Целью Федерального закона «О персональных данных» №152-ФЗ является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Действие закона не распространяется на отношения, возникшие при:

- обработке персональных данных физическими лицами исключительно для личных и семейных нужд;
- организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов;
- обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

Принципы обработки персональных данных:

1) законность целей и способов обработки персональных данных и добросовестности

2) соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных

3) соответствие объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных

4) достоверность персональных данных, их достаточность для целей обработки, недопустимость обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных

Принципы обработки персональных данных:

5) недопустимость объединения созданных для разных целей баз данных

6) хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки

7) Персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении

8) Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Условия обработки персональных данных:

обработка персональных данных осуществляется с согласия субъекта персональных данных;

обработка персональных данных необходима для достижения целей, предусмотренных международным договором РФ или законом;

обработка персональных данных необходима для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта.

Условия обработки персональных данных:

обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов РФ;

обработка персональных данных необходима для исполнения договора;

обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

Условия обработки персональных данных:

обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц, в том числе в случаях, предусмотренных ФЗ «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности», либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой;

Условия обработки персональных данных:

обработка персональных данных осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных;

осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных.

Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

Ответственность перед субъектом персональных данных за действия указанного лица несет оператор.

Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

Согласие на обработку персональных данных:

Субъект персональных данных дает согласие на их обработку свободно, своей волей и в своем интересе.

Согласие должно быть конкретным, информированным и сознательным.

Согласие может быть отозвано субъектом персональных данных.

В случае отзыва согласия оператор вправе продолжить обработку персональных данных без согласия при не выполнении целей обработки информации.

Структура согласия на обработку ПД:

Ф. И. О, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

наименование или Ф. И. О. и адрес оператора, получающего согласие субъекта персональных данных;

цель обработки персональных данных;

перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

Структура согласия на обработку ПД:

перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

подпись субъекта персональных данных.

Обработка специальных категорий персональных данных в ОУ, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается.

Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

Субъект ПД имеет право на получение следующей информации:

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- применяемые оператором способы обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором.

Субъект ПД имеет право на получение следующей информации:

- обрабатываемые персональные данные, источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или Ф. И. О. и адрес лица, осуществляющего обработку персональных данных по поручению оператора.

Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от:

неправомерного или случайного доступа;

уничтожения;

изменения;

блокирования;

копирования;

распространения персональных данных;

от иных неправомерных действий.

Меры, направленные на обеспечение выполнения оператором обязанностей по безопасной обработке ПД

1) назначение ответственного за организацию обработки персональных данных;

2) издание документов, определяющих политику оператора в отношении обработки персональных данных,

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных требованиям к защите персональных данных, локальным актам ОО;

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения ФЗ;

6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных

Меры по обеспечению безопасности персональных данных

1) определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн, необходимых для выполнения требований к защите ПД, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учет машинных носителей персональных данных;

Меры по обеспечению безопасности персональных данных

6) обнаружение фактов несанкционированного доступа к персональным данным и принятием мер по их устранению;

7) восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установление правил доступа к персональным данным, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Обязанности оператора при обращении к нему субъекта ПД

Оператор обязан сообщить субъекту ПД о наличии персональных данных, относящихся к соответствующему субъекту ПД, а также предоставить возможность ознакомления с этими ПД при обращении субъекта в течение тридцати дней с даты получения запроса субъекта ПД.

В случае отказа в предоставлении информации о наличии ПД о соответствующем субъекте оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение ч. 8 ст. 14 ФЗ № 152 или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных.

В срок, не превышающий семи рабочих дней со дня предоставления субъектом ПД сведений, подтверждающих, что ПД являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения.

В срок, не превышающий семи рабочих дней со дня представления субъектом ПД сведений, подтверждающих, что такие ПД являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие ПД.

Оператор обязан сообщить в уполномоченный орган по защите прав субъектов ПД по запросу этого органа необходимую информацию в течение тридцати дней с даты получения запроса.

Обязанности оператора по устранению нарушений законодательства

В случае выявления неправомерной обработки ПД оператор обязан осуществить блокирование неправомерно обрабатываемых ПД или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого выявления.

В случае подтверждения факта неточности ПД оператор на основании сведений, представленных субъектом ПД обязан уточнить ПД либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

В случае выявления неправомерной обработки ПД, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку ПД или обеспечить прекращение неправомерной обработки персональных данных.

В случае, если обеспечить правомерность обработки ПД невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПД, обязан уничтожить такие персональные данные или обеспечить их уничтожение.

Об устранении допущенных нарушений уведомить субъект ПД.

В случае достижения цели обработки ПД оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение и уничтожить ПД или обеспечить их уничтожение в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных.

В случае отзыва субъектом ПД согласия на обработку его ПД оператор обязан прекратить их обработку и в случае, если сохранение ПД более не требуется для целей обработки ПД, уничтожить ПД в срок, не превышающий тридцати дней с даты поступления указанного отзыва,

Ответственность за нарушение требований к обработке персональных данных:

-штраф;

-приостановление или даже прекращение обработки персональных данных;

-приостановление и аннулирование лицензии, в тех случаях, когда деятельность является лицензируемой;

Ответственность - лица, виновные в нарушении требований Федерального закона 152-ФЗ, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Содержание отдельных статей ФЗ “Об информации, информационных технологиях и защите информации” № 149 – ФЗ от 27.07.2006 г.

Закон регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;
- обеспечении защиты информации.

Основные понятия

- **информация** - сведения (сообщения, данные) независимо от формы их представления;
- **информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
- **информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

Основные понятия

обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Принципы правового регулирования отношений в сфере информации, ИТ и защиты информации:

- свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
- установление ограничений доступа к информации только федеральными законами;
- открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
- равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

Принципы правового регулирования отношений в сфере информации, ИТ и защиты информации:

обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

достоверность информации и своевременность ее предоставления;

неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних ИТ перед другими, если только обязательность применения определенных ИТ для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Вся информация делится на **общедоступную** и **ограниченного доступа**.

К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Категории информации в зависимости от порядка ее предоставления или распространения:

информация, свободно распространяемая;

информация, предоставляемая по соглашению лиц, участвующих в соответствующих отношениях;

информация, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

информация, распространение которой в Российской Федерации ограничивается или запрещается.

Оператор информационной системы в случаях, установленных законодательством РФ, обязаны обеспечить:

предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

своевременное обнаружение фактов несанкционированного доступа к информации;

предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

постоянный контроль за обеспечением уровня защищенности информации.