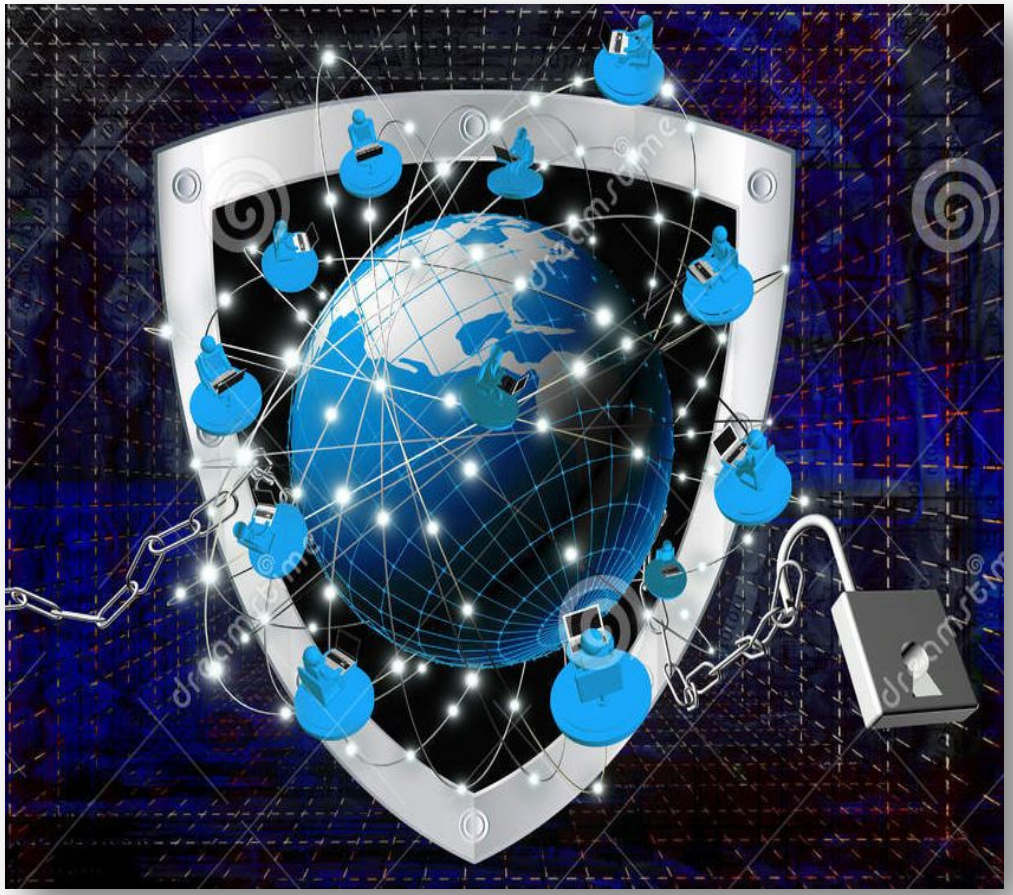
… то, что мы знаем – ограничено,
а то, что не знаем – бесконечно…

ПУСТЬ БУДЕТ ДОБРЫМ ИНТЕРНЕТ

К Всемирному Дню безопасности интернета и Неделе Рунета

Информационная безопасность



Безопасность – отсутствие угроз, либо состояние защищенности от угроз.

Информация – сведения или сообщения. Основные понятия

Угроза информационной безопасности – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства в информационной сфере.

Линия помощи «Дети онлайн» - служба телефонного и онлайн консультирования для детей и взрослых по проблемам безопасного использования детьми и подростками Интернета и мобильной связи. Полученные сигналы рассматриваются специалистами линии, при наличии достаточных оснований направляется уведомление провайдеру о прекращении оборота противоправного контента, а также инициируются правоохранительные процедуры. Если контент расположен за рубежом, информация передаётся на «Горячую линию» страны назначения в рамках сети INHOPE.

«Горячая линия» центра безопасного интернета в России в случае интернет-угроз

8-800-250-00-15 (с 9.00 до 18.00 по рабочим дням, время московское), звонки по России бесплатные.

helpline@detionline.com

www.detionline.com

Международные документы

"Конвенция о правах ребенка" (одобрена Генеральной Ассамблеей ООН 20.11.1989) (вступила в силу для СССР 15.09.1990)

Декларация принципов, принятая на Всемирном Саммите по Информационному обществу (Женева 2003 г. - Тунис 2005 г.)

План действий, принятый на Всемирном Саммите по Информационному обществу (Женева 2003 г. - Тунис 2005 г.)

Окинавская Хартия глобального информационного общества

Европейская Конвенция по киберпреступлениям (преступлениям в киберпространстве)

Рекомендация № R (97) 20 комитета министров государствам-членам по вопросам "разжигания ненависти"

Декларация Комитета министров Совета Европы о свободе выражения мнений и информации в СМИ в контексте борьбы с терроризмом (2005)

Рекомендация Парламентской Ассамблеи Совета Европы № 1706 (2005) "Средства массовой информации и терроризм»

Законы РФ

Закон РФ от 27.12.1991 N 2124-1 "О средствах массовой информации" (с изм. и доп., вступ. в силу с 01.08.2021)

Федеральный закон от 06.03.2006 N 35-ФЗ "О противодействии терроризму" (ред. от 26.05.2021)

Федеральный закон от 07.07.2003 N 126-ФЗ (ред. от 30.12.2021) "О связи" (с изм. и доп., вступ. в силу с 01.01.2022)

Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 30.12.2021) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.01.2022)

Федеральный закон от 29.12.2010 N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию"(ред. от 01.07.2021)

ПЯТЬ ПРАВИЛ БЕЗОПАСНОГО ПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТОЙ

1. Никогда не открывайте подозрительные сообщения или вложения электронной почты, полученные от незнакомых людей. Удалите их.
2. Никогда не отвечайте на спам.
3. Применяйте фильтр спама или программы работы с электронной почтой.
4. Создайте новый или используйте семейный адрес электронной почты для Интернет-запросов , дискуссионных форумов и т.д.
5. Никогда не пересылайте «письма счастья»

БЕЗОПАСНОСТЬ В ТВОИХ РУКАХ

НЕ сообщайте личную информацию (имя, адрес, телефон)

НЕ встречайтесь с кем-либо из он-лайн без разрешения родителей

НЕ открывайте электронное письмо от неизвестных отправителей

НЕ отправляйте свою фотографию по Интернету незнакомым людям.

Не сообщай информацию о себе в обмен на чтобы то ни было.

СОВЕТ:

Проводи больше времени с реальными друзьями

Расскажи взрослым о том, что тебя беспокоит в интернет-общении

ПРАВИЛА БЕЗОПАСНОГО ПОВЕДЕНИЯ В СОЦИАЛЬНЫХ СЕТЯХ

- Не заполняйте все поля вашего профиля.
- Не выкладывайте в социальных сетях откровенные фотографии.
- Не регистрируйтесь под чужими данными.
- Если хотите сохранить инкогнито – прибегните к вымышленному имени.
- Не используйте чужие изображения без разрешения этих людей.
- Никогда не используйте социальную сеть или иной подобный сервис в качестве основного хранилища информации.

ЗАЩИТИ СЕБЯ САМ

ЗАЩИТА ПАРОЛЕМ

- Используйте надёжный пароль. Его нужно правильно создавать, аккуратно хранить и регулярно менять.
- Выясните, какие программные способы предлагает владелец сети для защиты данных.
- Не забывайте очищать историю и удалять сохраненный пароль после работы со своим аккаунтом с чужого компьютера.

ЗАПОМНИТЕ 5 «НЕ»

- Не пишите в ленте о своих «подвигах», неправомерных с точки зрения закона.
- Не добавляйте в друзья всех подряд.
- Не вступайте в сомнительные сообщества, куда вас навязчиво приглашают.
- Не участвуйте в сомнительных акциях.
- Не переходите по длинным ссылкам, это чаще всего путь к зараженному вирусом файлу.

Соблюдайте культуру общения в сети.

ОТВЕТСТВЕННОСТЬ ЗА ИНФОРМАЦИОННЫЕ ПРАВОНАРУШЕНИЯ

Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма

от штрафа в размере до 500 тысяч рублей

до лишения свободы на срок от 2 до 5 лет.

Реабилитация нацизма

от штрафа до 300 тысяч рублей

до лишения свободы на срок до 3 лет.

Распространение личной или семейной тайны человека

От возмещения морального ущерба до лишения свободы на срок до 2 лет.

Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности России

От штрафа в размере от 100 до 300 тысяч рублей до лишения свободы на срок до 5 лет.

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ

гл. 28 «Преступления в сфере компьютерной информации» Уголовного Кодекса РФ Статья 272. Неправомерный доступ к компьютерной информации

От штрафа в размере до двухсот тысяч рублей

до лишения свободы на срок до семи лет.

Что в Интернете запрещено законом?

- Размещать информацию о себе
- Призывать к суициду
- Размещать информацию о других без их согласия
- Общаться
- Копировать файлы для личного использования
- Вести экстремистскую деятельность
- Осуществлять неправомерный доступ к закрытой информации
- Совершать покупки
- Создавать, использовать и распространять вредоносное ПО
- Участвовать в онлайн-опросах

МБУК АЦБС
имени князя Г.Е. Львова

СПАСИБО ЗА ВНИМАНИЕ

г. Алексин 2022