МКУ КМЦИКТ «СТАРТ»

ПОВЫШЕНИЕ УРОВНЯ ЗАЩИЩЕННОСТИ В ЦИФРОВОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ

Главный специалист
информационно-технологического отдела: А.А. Гузенко

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЕТЕЙ

Это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию.

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

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ -

“

комплекс организационных, технических и технологических мер по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе

УГРОЗА безопасности компьютерной системы

ВИДЫ ОНЛАЙН-УГРОЗ

ВИРУС

МОШЕННИЧЕСКИЕ ПИСЬМА

ПОЛУЧЕНИЕ ДОСТУПА К АККАУНТАМ В СОЦСЕТЯХ

ВИРУС

РЕКОМЕНДАЦИИ:

- использовать антивирусное программное обеспечение с обновленными базами вирусных сигнатур;
- регулярное обновление операционной системы;
- не открывать вложенные файлы или ссылки, полученные по электронной почте;
- обращать внимание на предупреждения браузера что сайт может угрожать безопасности компьютера.

Создание и распространение вредоносных программ (в том числе вирусов) преследуется в России согласно Уголовному кодексу РФ (глава 28, статья 273)

МОШЕННИЧЕСКИЕ ПИСЬМА

РЕКОМЕНДАЦИИ:

- внимательно изучить информацию из письма;
- проверить достоверность описанных фактов;
- если в письме предлагается большая выгода за незначительное вознаграждение, скорее всего, оно мошенническое;
- проверять адрес отправителя на предмет соответствия официальному адресу отправителя;
- осуществлять проверку вложений, содержащихся в электронных письмах средствами антивирусной защиты до их открытия.

ПОЛУЧЕНИЕ ДОСТУПА К АККАУНТАМ В СОЦСЕТЯХ

РЕКОМЕНДАЦИИ:

- использовать сложные пароли *(состоят как минимум из 10 символов);*
- никому не сообщать свой пароль;
- не передавать учетные данные – логины и пароли – по незащищенным каналам связи;
- внимательно проверять доменные имена сайтов, на которых вводятся учетные данные.

ПРАВОВАЯ ОСНОВА

системы защиты информации

- Конституция РФ
- Доктрина информационной безопасности РФ
- Федеральные законы РФ
- Указы и распоряжения Президента РФ
- Постановления Правительства РФ

НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ безопасности персональных данных

- Федеральный закон от 27.07.2006 N 152-ФЗ
- Федеральный закон от 19.12.2005 N 160-ФЗ
- Постановление Правительства РФ от 01.11.2012 N 1119
- Постановление Правительства РФ от 06.07.2008 N 512
- Постановление Правительства РФ от 15.09.2008 N 687
- Постановление Правительства РФ от 21 марта 2012 года N 211

ВИДЫ ЗАЩИТЫ ИНФОРМАЦИИ

ОРГАНИЗАЦИОННАЯ ЗАЩИТА

ТЕХНИЧЕСКАЯ ЗАЩИТА

ПРОГРАММНАЯ ЗАЩИТА

ОРГАНИЗАЦИОННАЯ ЗАЩИТА

- организация режима и охраны
- организация работы с сотрудниками
- организация работы с документами
- организация использования технических средств
- организация работы по анализу внутренних и внешних угроз
- организация работы по проведению систематического контроля за работой персонала

ОСНОВНЫЕ ДОКУМЕНТЫ по информационной безопасности

- Политика в области обработки персональных данных;
- Положение об обработке (защите) персональных данных;
- Согласие работника на обработку персональных данных;
- Согласие работника на распространение персональных данных;
- Обязательство о неразглашении персональных данных;
- Парольная политика;
- Приказ об утверждении внутренних нормативных актов по защите информации;
- Приказ о назначении ответственного за организацию обработки персональных данных и администратора безопасности информации;
- Инструкция администратора безопасности;
- Инструкция ответственного за организацию обработки персональных данных

ТЕХНИЧЕСКАЯ ЗАЩИТА

Для защиты периметра информационной системы создаются:

- системы охранной и пожарной сигнализации
- системы цифрового видео наблюдения
- системы контроля и управления доступом (СКУД)

ТЕХНИЧЕСКАЯ ЗАЩИТА

Системы бесперебойного питания:

- источники бесперебойного питания
- резервирование нагрузки
- генераторы напряжения

ТЕХНИЧЕСКАЯ ЗАЩИТА

Защита от утечки информации техническими каналами связи обеспечивается следующими средствами и мероприятиями:

- использованием экранированного кабеля и прокладки проводов и кабелей в экранированных конструкциях
- установкой на линиях связи высокочастотных фильтров
- использованием экранированного оборудования
- созданием контролируемых зон

ПРОГРАММНАЯ ЗАЩИТА

- средства защиты от несанкционированного доступа (НСД);
- системы анализа и моделирования информационных потоков;
- инструментальные средства анализа систем защиты;
- системы мониторинга сетей;
- антивирусные средства;
- межсетевые экраны;
- системы резервного копирования;
- системы аутентификации

Статья	Нормативно-правовой акт	Нарушение	Мера наказания
13.11 (ч.2)	КоАП РФ	Обработка ПДн без письменного согласия субъекта	Штраф от 20 000 до 40 000 рублей За повторное нарушение – от 40 000 до 100 000 рублей
13.11 (ч.4)	КоАП РФ	Невыполнение обязанности по предоставлению субъекту ПДн информации, касающейся обработки его ПДн	Штраф от 8 000 до 12 000 рублей
13.11 (ч.5)	КоАП РФ	Невыполнение оператором в сроки, установленные законодательством, требования об уточнении ПДн, их блокировании или уничтожении	Штраф от 8 000 до 20 000 рублей За повторное нарушение – от 30 000 до 50 000 рублей
81 (ч.6 п.в), 193	ТК РФ	Разглашение ПДн, ставших известными работнику в связи с исполнением им трудовых обязанностей	Увольнение
90, 193	ТК РФ	Ответственность за нарушение норм, регулирующих обработку и защиту ПДн работника	Замечание Выговор Увольнение Материальная ответственность

СПАСИБО
ЗА ВНИМАНИЕ!

ПОЧТОВЫЙ АДРЕС

г. Краснодар, ул. Коммунаров, д. 119

ЭЛЕКТРОННЫЙ АДРЕС

centerstart@kubannet.ru

НОМЕР ТЕЛЕФОНА

+7 (861) 255-84-46