Информационная безопасность

03.10.2014

1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ.

Информационная безопасность – защищенность информации и соответствующей инфраструктуры от случайных или преднамеренных воздействий сопровождающихся нанесением ущерба владельцам или пользователям информации.

Информационная безопасность – обеспечение конфиденциальности, целостности и доступности информации.

Цель защиты информации – минимизация потерь, вызванных нарушением целостности или конфиденциальности данных, а также их недоступности для потребителей.

2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Основные типы угроз информационной безопасности:

1. Угрозы конфиденциальности – несанкционированный доступ к данным.

2. Угрозы целостности – несанкционированная модификация, дополнение или уничтожение данных.

3. Угрозы доступности – ограничение или блокирование доступа к данным.

Источники угроз:

1. Внутренние:

а) ошибки пользователей и сисадминов;

б) ошибки в работе ПО;

в) сбои в работе компьютерного оборудования;

г) нарушение сотрудниками компании регламентов по работе с информацией.

2. Внешние угрозы:

а) несанкционированный доступ к информации со стороны заинтересованных организаций и отдельных лица;

б) компьютерные вирусы и иные вредоносные программы;

в) стихийные бедствия и техногенные катастрофы.

3. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ.

Методы обеспечения безопасности информации в ИС:

- **Препятствие —** физическое преграждение пути злоумышленнику к защищаемой информации .
- **Управление доступом –** регулирование использования информации и доступа к ней за счет системы идентификации пользователей, их опознавания, проверки полномочий и т.д.
- **Криптография –** шифрование информации с помощью специальных алгоритмов.
- **Противодействие атакам вредоносных программ –** предполагает использование внешних накопителей информации только от проверенных источников, антивирусных программ, брандмауэров, регулярное выполнение резервного копирования важных данных и т.д. (*вредоносных программ очень много и они делятся на ряд классов: вирусы, эксплойты, логические бомбы, трояны, сетевые черви и т.п.*).
- **Регламентация –** создание условий по обработке, передаче и хранению информации, в наибольшей степени обеспечивающих ее защиту (*специальные нормы и стандарты для персонала по работе с информацией, например, предписывающие в определенные числа делать резервную копию электронной документации, запрещающие использование собственных флеш-накопителей и т.д.*).
- **Принуждение –** установление правил по работе с информацией, нарушение которых карается материальной, административной или даже уголовной ответственностью (*штрафы, закон «О коммерческой тайне» и т.п.*).
- **Побуждение –** призыв к персоналу не нарушать установленные порядки по работе с информацией, т.к. это противоречит сложившимся моральным и этическим нормам.

Средства защиты информации:

- **Технические (аппаратные) средства –** сигнализация, решетки на окнах, генераторы помех воспрепятствования передаче данных по радиоканалам, электронные ключи и т.д.

- **Программные средства** – программы-шифровальщики данных, антивирусы, системы аутентификации пользователей и т.п.
- **Смешанные средства** – комбинация аппаратных и программных средств.
- **Организационные средства** – правила работы, регламенты, законодательные акты в сфере защиты информации, подготовка помещений с компьютерной техникой и прокладка сетевых кабелей с учетом требований по ограничению доступа к информации и пр.

НОРМАТИВНО-ПРАВОВАЯ БАЗА

1. Федеральный закон РФ от 27.07.2006 г. № 152 — ФЗ «О персональных данных»
2. Федеральный закон РФ от 28.12.2010 г. № 390 — ФЗ «О безопасности»
3. Федеральный закон РФ от 29.12.2010 г. № 436 — ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»
4. Указ Президента РФ от 04.03.2013 г. № 183 «О рассмотрении общественных инициатив, направленных гражданами Российской Федерации с использованием интернет-ресурса «Российская общественная инициатива»

ЛОКАЛЬНЫЕ ДОКУМЕНТЫ ДОУ

1. Положение об использовании сети Интернет и электронной почты в МДОУ «Детский сад 2».
2. Положение по организации парольной защиты в МДОУ «Детский сад № 2».
3. Приказ «Об использовании сети интернет и электронной почты».
4. Приказ «Об утверждении положения по организации парольной защиты».
5. Согласие на обработку персональных данных.
6. Согласие на проведение видео и фотосъемки.

СОВЕТЫ РОДИТЕЛЯМ:

1. Информационная безопасность детей

— это состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и

(или) физическому, психическому, духовному, нравственному развитию.

Согласно Закону № 436 – ФЗ информацией, причиняющей вред здоровью и (или) развитию детей, является:
— информация, запрещенная для распространения среди детей;
— информация, распространение которой ограничено среди детей определенных возрастных категорий.

К информации запрещенной для распространения среди детей, относится:

1) информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью;
2) способность вызвать у детей желание принять участие в азартных играх, заниматься бродяжничеством или попрошайничеством;
3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям и животным;
4) отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
5) оправдывающая противоправное поведение;
6) содержащая нецензурную брань.
К информации, распространение которой ограничено среди детей определенного возраста, относится:

1) информация, 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 т.ч. 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.

В Интернете ребенок старается посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям (законным представителям) особенно полезны будут те отчеты, которые предоставляются программами по ограничению использования Интернета, т. е. Родительский контроль или то, что вы сможете увидеть во временных файлах Интернета. В результате, у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако, родители будут по-прежнему знать, какие сайты посещает их ребенок. Дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Они любят играть в сетевые игры и путешествовать по Интернет, используя электронную почту, заходить на сайты и чаты, не рекомендованные родителями.

2.Советы по безопасности в сети Интернет для детей

- Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.
- Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что вы наблюдаете за ним не потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.
- Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
- Используйте специальные детские поисковые машины.
- Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
- Создайте семейный электронный ящик чтобы не позволить детям иметь собственные адреса.
- Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего ПО.
- Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами

электронной почты, в чатах, регистрационных форм и профилей.

- Научите детей не загружать файлы, программы или музыку без вашего согласия.
- Не разрешайте детям использовать службы мгновенного обмена сообщениями.
- В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.

Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.