СВОД ПРАВИЛ ПО БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ СЕТИ ИНТЕРНЕТ

ПОНЯТИЙНЫЙ АППАРАТ

Контент (от английского content - содержание) – это любое информационно значимое либо содержательное наполнение информационного ресурса или веб-сайта: тексты, мультимедиа, графические изображения.

Как одну из разновидностей контента выделяют мобильный контент. Под мобильным контентом подразумевают цифровой контент, который адресован владельцам мобильных устройств.

В качестве мобильного контента чаще всего можно встретить:

- **текстовые файлы;**
- **цифровые картинки, (допустим, в формате .gif или .jpg и прочие);**
- **звуковые файлы (.midi, mp3 и прочие);**
- **видеофайлы (.avi, .mp4, .mpeg и прочие)**
- **а также другие цифровые файлы, которые можно загружать в мобильные устройства при помощи беспроводной связи.**

! **Весь контент в Интернете охраняется законом об авторских правах, являясь продуктом интеллектуального труда, имеет авторов и владельцев.**

РИСКИ (УГРОЗЫ) ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. **КОНТЕНТНЫЕ РИСКИ.**
   Нарушение авторского права, пропаганда экстремизма и наркотиков, порнография, детская порнография, нецензурные тексты.
2. **НАРУШЕНИЯ БЕЗОПАСНОСТИ.**
   Вирусы, трояны, нежелательная почта (спам), онлайн мошенничества.
3. **КОММУНИКАЦИОННЫЕ РИСКИ.**
   Незаконный контакт, киберпреследование (угрозы, сексуальные домогательства с использованием информационных технологий).

ПОНЯТИЙНЫЙ АППАРАТ

Троя́нская программа (также — троя́н, троя́нец, троя́нский конь) — вредоносная программа, распространяемая людьми, в отличие от других вирусов и червей, которые распространяются самопроизвольно. В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и её передачу злоумышленнику, её разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.

ПУТИ РАСПРОСТРАНЕНИЯ

Анализ случаев заражения показал, что основными путями распространения вредоносных компьютерных программ (далее – компьютерные вирусы) являются:

- - канал электронной почты, активируется открытием вложений к письму;
- - веб-серфинг на автоматизированных рабочих местах с доступом к сети Интернет, при скачивании пользователем контента в виде самораспаковывающихся архивов на посторонних ресурсах;
- - неконтролируемое использование неучтенных магнитных носителей информации (далее – флешка, МНИ);
- - самостоятельно устанавливаемое пользователем нелицензионное программное обеспечение.

ПОСЛЕДСТВИЯ ЗАРАЖЕНИЯ КОМПЬЮТЕРА

- Приостановка деятельности пользователя до восстановления работоспособности ПЭВМ службой технической поддержки;
- Нарушение нормального функционирования информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации на АРМ;
- Уничтожение, повреждение или разрушение средств и систем обработки информации, телекоммуникации и связи, подключаемых машинных и других носителей информации;
- Воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- Перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
- Несанкционированный доступ к информации, находящейся в банках и базах данных;
- Внедрение в программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- Нарушение законных ограничений на распространение информации.

Особые опасности (для продвинутых моделей вирусного программного обеспечения, ориентированных на базы данных, либо портированных с мобильных устройств на операционные системы семейства Windows):

- **противоправные сбор и использование информации;**
- **нарушения технологии обработки информации;**
- **компрометация ключей (электронных подписей) и средств криптографической защиты информации;**
- **утечка информации по техническим каналам.**

ПРИЗНАКИ ЗАРАЖЕНИЯ КОМПЬЮТЕРА

- **Компьютер работает необычно медленно.**
- **Внезапно появляются всплывающие окна с нежелательным содержимым (реклама, «взрослые» сайты и тому подобное).**
- **Многократное аварийное завершение работы приложений или всего компьютера (иногда даже с появлением «синего экрана»).**
- **Подозрительно активная работа жёсткого диска компьютера.**
- **Неожиданно быстро закончилось (заканчивается) свободное место на жёстком диске.**
- **Необычно высокая сетевая активность компьютера.**
- **Смена в браузере страницы, загружаемой по умолчанию, появление в браузере новых панелей инструментов, которые вы не ставили, а в истории посещений браузера - страниц, которые вы не посещали.**
- **Появление неизвестных диалоговых окон (в том числе в процессе загрузки компьютера), самопроизвольная загрузка и закрытие приложений, уведомление Windows об отсутствии доступа к какому-либо из локальных дисков.**
- **Антивирус отключён полностью или отключена функция его обновления.**
- **Ваши коллеги, знакомые и/или родственники сообщают, что получили от вас сообщения, которых вы не отправляли**

ПРАВИЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Используйте надежный пароль
2. Периодическим меняйте пароли на самых важных ресурсах (сайтах.
3. Заведите не менее двух почтовых адресов: основной и вспомогательный
4. Скачивайте программы с официальных сайтов разработчиков
5. Для скачивания контента не с сайтов разработчиков программного обеспечения или других официальных сайтов пользуйтесь одноразовыми почтовыми ящиками.
6. Не нажимайте на красивые баннеры или рекламные блоки на сайтах, какими бы привлекательными и заманчивыми они не были
7. Не сохраняйте пароли в браузере
8. Не открывайте письма от неизвестных Вам пользователей.
9. Не нажимайте на вплывающие окна, оповещающие о блокировке вашей учетной записи в социальных сетях
10. Заходите в сеть Интернет только при наличии на компьютере: актуальных обновлений операционной системы, настроенных антивируса с обновлёнными базами сигнатур вирусов и включенного файервола (межсетевого экрана)

ПРАВИЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ в отпуске

1. Выключайте wi-fi-модуль, если не пользуетесь им – тем самым вы и снизите риск кражи данных, и сбережёте заряд батареи устройства.
2. С подозрением относитесь к незапароленным беспроводным сетям – такие сети часто используются злоумышленниками для сбора данных.
3. Не пользуйтесь онлайн-банком и другими критически важными сервисами если не уверены в безопасности подключения. Если использование онлайн-банка действительно необходимо, менее рискованно использовать мобильный интернет.
4. Там, где возможно, используйте подключение по защищённому протоколу HTTPS. Например, его можно использовать для поиска в Google, Wikipedia и для Facebook. Для использования этого протокола в социальной сети «ВКонтакте» необходимо в настройках проставить галочку «Всегда использовать безопасное соединение».
5. Для интернет-сёрфинга с помощью браузеров Chrome, FireFox и Opera установите специальное расширение браузера HTTPS Everywhere (https://www.eff.org/HTTPS-EVERYWHERE), обеспечивающее более безопасную передачу данных.
6. Если возможно, используйте VPN-соединения. Это обычно платная услуга, но она обеспечивает эффективную защиту от перехвата трафика и взлома устройств.
7. Включите функцию шифрования данных вашего устройства.
8. Установите современное антивирусное и антивредоносное ПО и не забывайте обновлять его вирусную базу.

ЦИТАТЫ

Распоряжение Правительства Ульяновской области от 04.02.2015 №43-пр «Об утверждении Правил пользования локальной вычислительной сетью Правительства Ульяновской области» (в редакции распоряжения Правительства Ульяновской области №732-пр от 26.12.2016)

4.3.3. Срок действия пароля не превышает 90 календарных дней. Пароль не может быть использован повторно при истечении его срока действия.

4.3.4. Пароль должен соответствовать следующему уровню сложности:
длина пароля не менее 9 символов;
наличие не менее одной заглавной буквы;
наличие не менее одной цифры;
наличие не менее одного псевдосимвола;
пароль не должен содержать слово на каком-либо языке, написанное в соответствии с правилами и грамматикой языка.

4.3.5. Пользователь обязан хранить пароль доступа к информационным системам ЛВС в тайне и не сообщать его другим лицам.

В случае компрометации пароля пользователь должен незамедлительно известить об этом факте Оператора ЛВС и ОЗИ.

ПРИМЕР ХОРОШЕГО ПАРОЛЯ

Пользователям с «плохой памятью» рекомендуется…

Для создания ХОРОШЕГО пароля[1] понадобится:

1. Песня (стихотворение, пословица), которую вы знаете наизусть
2. Немного фантазии
3. «Своё» правило запоминания

Вместе весело шагать

В латинской раскладке это выглядит так:

Dvtcnt dtctkj ifufnm

Берём из каждого слова 3 буквы, например, из 1 слова – с первого символа по третий, из 2 слова – со второго символа по четвертый, из 3 слова – с третьего символа по шестой.

Dvtcnt d**tct**kj if**ufn**m

Получили 3 группы знаков:

Dvt tct ufn

Усложняем

Dvt tCt ufN

Добавляем цифры

Dvt2tCt5ufN

Добавляем псевдосимволы (спецсимволы), например: ! @ # $ % ^ & () - _ = +

!Dvt2tCt5ufN#

[1] для сетевых аккаунтов рекомендуемая длина пароля **от 12 символов**

!Dvt2tCt5ufN#

!Dvt2tCt5ufN#

!Dvt2tCt5ufN#

СПАСИБО ЗА ВНИМАНИЕ

!Dvt2tCt5ufN#

!Dvt2tCt5ufN#

!Dvt2tCt5ufN#