



№ _____

На № _____ от _____

**Руководителям органов образования
исполнительных комитетов
муниципальных образований
Республики Татарстан**

Об информационной безопасности

В целях обеспечения информационной безопасности в руководимых Вами управлениях (отделах) и образовательных организациях Министерство образования и науки Республики Татарстан рекомендует открывать бюджетные и внебюджетные лицевые счета получателей бюджетных средств в «Ак Барс» банке.

Направляем Вам для учета в работе презентационные материалы и памятку по итогам семинара по вопросам информационной безопасности, предоставленные Министерством информатизации и связи Республики Татарстан.

Просим довести данное письмо до подведомственных организаций.

Приложение: 1. Презентация на 15 л.;
2. Памятка на 2 л.

**Заместитель Премьер-министра
Республики Татарстан – министр**

Э.Н. Фаттахов

Л.И. Кудрявцева
тел.(843)294-95-21



СОВРЕМЕННАЯ КИБЕРПРЕСТУПНОСТЬ

|GROUP|IB|

ПОЧЕМУ СУЩЕСТВУЕТ КИБЕРПРЕСТУПНОСТЬ?



ДЕНЬГИ



ИНФОРМАЦИЯ



МИРОВОЕ ГОСПОДСТВО - ТЕРРОРИЗМ

АКТУАЛЬНЫЕ КИБЕРУГРОЗЫ ДЛЯ ГОСУДАРСТВА

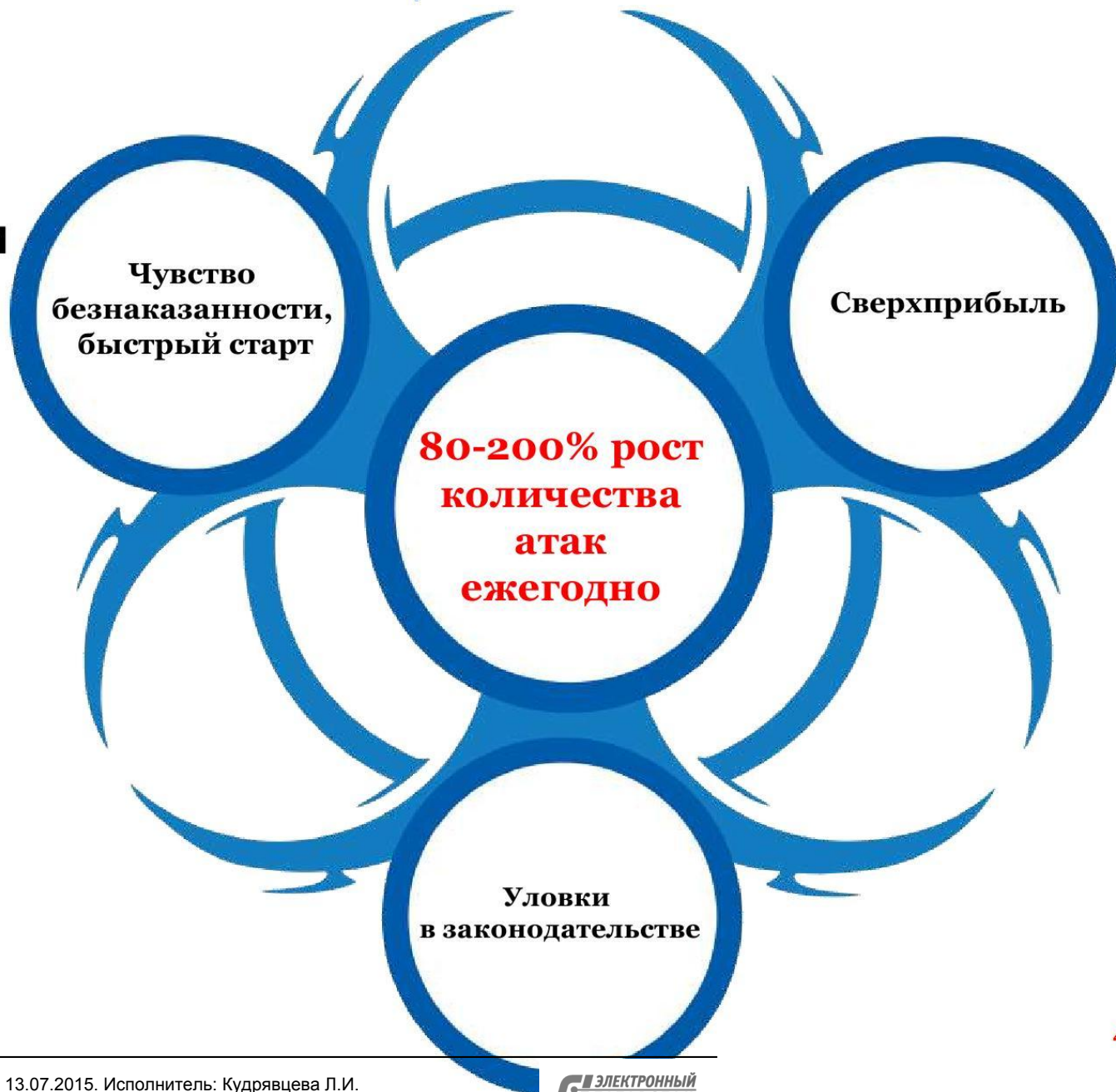
Терроризм
и экстремизм

Атаки на объекты
критически важной
для государства
инфраструктуры

Перехват управления
ключевыми
государственными
информационными
ресурсами

Кибершпионаж и
разглашение
государственной
тайны

Спрут киберпреступности



НЕДОПУСТИМЫЕ ФАКТЫ

8 из 10

предприятий и ведомств не знают,
что их сети взломаны

> 600

дней действия злоумышленников
остаются незамеченными

В 90%

случаев меры по предотвращению
подобных ситуаций не принимаются

Факты несанкционированного
доступа часто остаются
без внимания

Защита

5 простых правил

1е правило

Подумайте, прежде чем действовать:

опасайтесь сообщений, которые призывают действовать немедленно, предлагают что-то, что звучит слишком хорошо, чтобы быть правдой, или просят предоставить личную и информацию или что-то нажать



1234

+79512737287

Ваша Банковская
карта VISA
заблокирована
ИНФО+7-951-273-
72-87.

Функции Ответить

Назад

2е правило

Хорошо подумайте перед тем как ставить новое незнакомое приложение, скачивать музыку и фильмы

Остерегайтесь отправлять свою личную или конфиденциальную информацию

Не нажимайте на ссылки и не открывайте файлы от незнакомых людей (или даже от знакомых, если Вы не ждете этого-позвоните и спроси отправлял ли Вам этот файл)

Аккуратно общайтесь с незнакомцами онлайн

Если есть сомнения, не подключайтесь:
ссылки в электронной почте, заметки в
социальных сетях, сообщения и интернет-реклама зачастую создают киберпреступниками.

ADOBE FLASH PLAYER 10

FEATURES



ASTRO

GPU COMPOSITING

GPU SURFACING

DYNAMIC STREAMING

DRAWING API

NEW TEXT ENGINE

NATIVE 3D

INVERSE KINEMATICS

CUSTOM EFFECTS

ASTRO

To view this experience, you need
the latest version of
Adobe Flash Player Beta installed.

DOWNLOAD NOW

*CODENAME: ASTRO

3е правило

ПАРОЛЬНАЯ ЗАЩИТА

Создавайте
длинные и сложные пароли: комбинации букв с цифрами и символами
создают более безопасный пароль.

Новая учетная запись, уникальный пароль:
во вновь создаваемом пароле комбинируйте
буквы, цифры, верхний и нижний регистр;

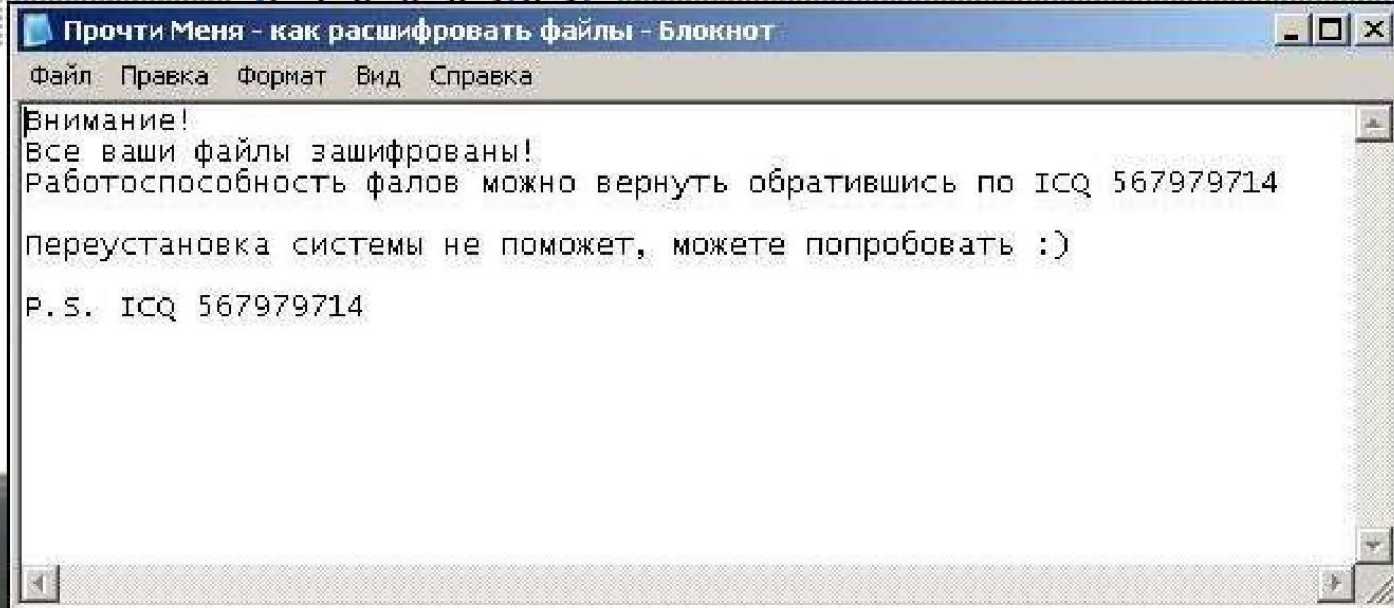
Можно использовать стихотворения и строчки песен для паролей - пиши
на английском, смотрите на русские буквы;

Пример:

Zdfck.,bkk.,jdmtot,snmvj;tn!

4е правило

Все, что Вы загружаете в интернет,
включая видео и фото - может стать
доступно всем и остаться с
Интернете навсегда



5е правило

Делайте резервные копии

ПАМЯТКА

- Блокируйте свой телефон и используйте хороший пароль;
- Не говорите пароль никому;
- Обновляйте операционную систему устройства и установленные приложения;
 - Настройте автоматические обновления: многие программы автоматически подключаются и обновляются. Это позволяет защитить систему от новых угроз;
 - Выключайте Wi-Fi, bluetooth, геолокацию – когда ими не пользуетесь;
 - Хорошо подумайте, перед тем как ставить новое незнакомое приложение, скачивать музыку и фильмы;
 - Остерегайтесь отправлять свою личную или конфиденциальную информацию;
 - Не нажимайте на ссылки и не открывайте файлы от незнакомых людей (или даже от знакомых, если вы не ждете этого – позвоните и спросите отправлял ли Вам коллега письмо);
 - Аккуратно общайтесь с незнакомцами онлайн;
 - Если есть сомнения, не подключайтесь: ссылки в электронной почте, заметки в социальных сетях, сообщения и Интернет-реклама зачастую создаются киберпреступниками;
 - Если письмо выглядит подозрительно, даже если вы знаете адресата, лучше удалите письмо, если это уместно, отметьте, как нежелательную почту/спам;
 - Следите за защищённостью учетных записей: многие ресурсы предлагают дополнительные способы идентификации, чтобы удостовериться кто вы (например, привяжите учетную запись к телефону и используйте двухфакторный вход – пароль+SMS пароль); Это нужно включить в социальной сети, почте и облачном хранилище данных (например, iCloud);
 - Создавайте длинные и сложные пароли: комбинации букв с цифрами и символами создают более безопасный пароль;
 - Новая учетная запись, уникальный пароль: во вновь создаваемом пароле комбинируйте буквы, цифры, верхний и нижний регистр. Можно использовать стихотворения и строчки песен для паролей – пишите на английском, смотрите на русские буквы;
 - Знайте об основных способах кражи информации и угрозах информационной безопасности. Идти в ногу со временем – лучший способ оставаться в безопасности в Интернете;
 - Спрашивайте разрешения своих друзей и коллег, чтобы поделиться их фотографиями и любой другой информацией о них;

- Знайте, что любой текст, который вы отправите, может стать доступен всем – подумайте об этом дважды;
- Все, что вы загружаете в Интернет, включая видео и фото – может стать доступно всем и остаться в Интернете навсегда;
- Подумайте, прежде чем действовать: опасайтесь сообщений, которые призывают Вас действовать немедленно, предлагают что-то, что звучит слишком хорошо, чтобы быть правдой, или просят предоставить личную информацию;
- Делайте резервные копии каждую неделю: электронная копия должна содержать файлы, почту, музыку, фото и другую цифровую информацию. Сделайте резервную копию и храните ее в безопасном месте (не на своем компьютере). Это касается как компьютера, так и мобильного телефона.

Лист согласования			Тип согласования: последовательное	
N°	ФИО	Срок согласования	Результат согласования	Замечания
1	Садыкова В.Р.		Согласовано 13.07.2015 - 13:22	-
2	Каюмов А.М.		 Согласовано 13.07.2015 - 15:26	-
3	Фаттахов Э.Н.		 Подписано 13.07.2015 - 23:48	-