Утверждаю
Руководитель Администрации
МО «Кяхтинский район»
_____ А.Ю. Фомин
«___» _____ 2024 г.

ПОЛОЖЕНИЕ

о проведении конкурса видеороликов по профилактике IT-преступлений

г. Кяхта
2024 г.

I. Общие положения

1.1. Организатором конкурса видеороликов по профилактике IT-преступлений, (далее – Конкурс), является Администрация МО «Кяхтинский район».

1.2. Настоящее Положение определяет цели и задачи, категории участников, порядок проведения и подведения итогов Конкурса.

1.3. Организационное, информационное и материально-техническое обеспечение Конкурса осуществляет Администрация МО «Кяхтинский район».

II. Цели и задачи Конкурса

2.1. Цель Конкурса – привлечение молодежи к созданию креативных видеороликов, а также распространение и информирование о возможных способах преступлений в сфере компьютерной информации.

2.2. Задачами Конкурса являются:

- пропаганда недопущения преступлений в сфере информационных технологий;
- привлечение внимания молодежи и вовлечение в медиа творчество;
- предоставление возможности для реализации творческих способностей;

III. Условия проведения Конкурса

3.1. Участниками Конкурса могут быть школьники и студенты образовательных учреждений Кяхтинского района.

3.2. Жанр видеоролика (видеоклип, документальный фильм, рекламный ролик) определяется участником (командой) самостоятельно. Хронометраж видеоролика должен быть ***не более 1,5 минут.***

3.3. К участию в Конкурсе принимаются работы, ранее нигде не опубликованные.

3.4. Участие в Конкурсе означает согласие автора на последующее некоммерческое использование его работ с указанием имени автора работы.

3.5. К участию в Конкурсе не допускаются работы, содержащие:

- нарушение требований к содержанию и оформлению конкурсных работ;
- ненормативную лексику;
- политические, религиозные и национальные разногласия.

IV. Порядок проведения Конкурса

4.1. Пакет документов и авторские работы предоставляются на E-mail: mol.politika.kyahta@mail.ru .

4.2. Сроки предоставления конкурсных работ ***до 25 января 2024 года***.

V. Конкурсная комиссия

5.1 В целях достижения максимальной объективности в определении победителей Конкурса создается Конкурсная комиссия, которая формируется организатором Конкурса.

5.2. Комиссия:

- проводит проверку работ участников Конкурса, оценивает их результаты;
- определяет победителей и распределяет призовые места.

5.3. Заседание Комиссии считается правомочным, если в нем принимает участие большинство от установленного количества членов.

5.4. Решение Комиссии принимается большинством голосов от числа её членов, присутствующих на заседании.

VI. Подведение итогов и награждение победителей Конкурса

6.1. Оценивание работ проводится по пятибалльной системе с учетом требований, указанных в данном Положении.

Оцениваются:

– творческий подход и оригинальный стиль работы;

– полнота раскрытия темы;
– образность и эмоциональность;
6.2. Итоговая оценка каждого участника (команды) формируется путем суммирования оценок всех членов Комиссии.
6.3. Победителем Конкурса признаётся участник (команда) набравший(ая) наибольшую сумму баллов.
6.4. Результаты Конкурса пересмотру не подлежат.
6.5. Победителей Конкурса определят 26 января 2024 года.
6.6. Победитель и призеры Конкурса награждаются грамотами и денежными призами.
6.7. По итогам Конкурса работы могут быть опубликованы в группе «Молодёжь Кяхты» в ВК https://vk.com/club223915607 .

VII. Соблюдение авторских прав

7.1. Организаторы Конкурса оставляют за собой право использовать любые конкурсные работы для освещения Конкурса, использовать конкурсные работы в некоммерческих проектах.

По вопросам обращаться по тел. 89516203570 (Шубина Светлана Сергеевна)

Информация
по профилактике ИТТ-преступлений для граждан

Способы ИТТ преступлений:

Преступления, совершаемые с использованием пластиковых банковских карт путем набора пин – кода, либо бесконтактным способом (wi-fi).

Примеры:

1. гр. Н., обнаружив в общественном месте, утерянную неизвестным лицом, банковскую пластиковую карту (с возможностью оплаты без ввода пин–кода) совершил с ее помощью покупку на сумму 1 000 рублей.

2. Преступник совершил кражу сумки, в которой находились документы и банковская карта (с записанным в документах пин - кодом). После чего совершает снятие денежных средств с банковской карты через банкомат, либо совершает по карте покупки.

Меры по обеспечению безопасности банковской карты

1 необходимо принять более тщательные меры по обеспечению сохранности личных банковских карт, пин-коды к ним хранить отдельно.

2. позвонить на «горячую линию» своего банка (номер указывается на обратной стороне банковской карты).

3. лично обратиться в ближайшее отделение банка и позвонить в дежурную часть ОВД (102 или 112).

Преступления, при совершении которого преступник использует устройство с возможностью выхода в сеть «Интернет», где формируются:

1) сайт-двойник, визуально похожий на какой-либо известный официальный сайт.

2) при использовании специальных программ удаленного доступа – мошенники при общении с гражданами убеждают последних установить «антивирусы», «безопасные программы», которые на самом деле являются программами, позволяющие управлять устройством гражданина дистанционным способом, после чего похищают деньги, находящиеся на счету граждан («RustDesk», «TeamViewer», «AnyDesk»).

Пример: гр. Н. в социальной сети «N» увидела объявление о покупке товаров и услуг по выгодной цене. Далее гр. «Н» переводит денежные средства преступнику, который в дальнейшем перестает ей отвечать, при этом, объявление блокируется.

Действия граждан

1. Чтобы не попасть, при оказании услуг, насайт-двойник обращайтесь к проверенным ранее Интернет-ресурсам, либо знакомым, родственникам и другим лицам, которые могут подтвердить достоверность официального сайта.

2. При поступлении звонка и разговора с неизвестными лицами о деньгах – прекратить телефонный разговор и позвонить в дежурную часть ОВД (102 или 112).

3. Не переходить по неизвестным ссылкам.

Преступления, совершаемые с использованием сотового телефона, с которого преступник осуществляет звонок потерпевшему, и обманным путём вынуждает последнего перевести ему денежные средства. Данный способ может применяться для **краж** и **мошенничеств**.

Пример:

гр. Н. поступает телефонный звонок от преступника, который представляется сотрудником службы безопасности банка. В ходе телефонного разговора преступник сообщает потерпевшему о том, что его банковская карта заблокирована, и для сохранения денежных средств, находящихся на банковском счете, ему необходимо осуществить их перевод на «безопасный» счет. Потерпевший, боясь за свои сбережения, осуществляет перевод денежных средств преступнику.

Действия граждан

1. При поступлении звонка и разговора с неизвестными лицами о деньгах – прекратить телефонный разговор и позвонить в дежурную часть ОВД (102 или 112).

2. При общении с неустановленными лицами по сети Интернет – не передавать поступающие коды и персональные данные из SMS-сообщений.