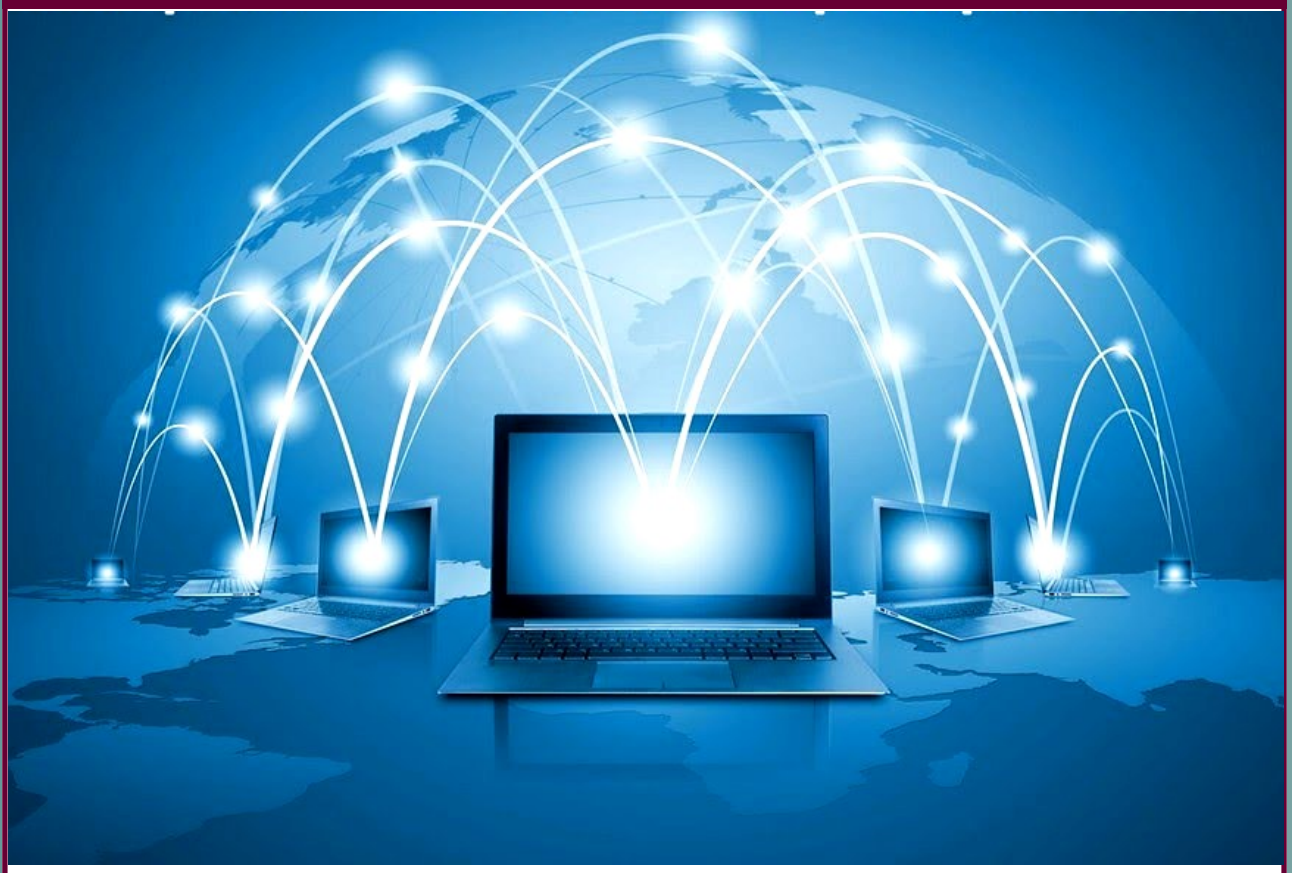
ИНТЕРНЕТ-БЕЗОПАСНОСТЬ

МБУ ДО “ДДТ “Дриада”



Большая часть нашей повседневной жизни так или иначе связана с интернетом. С ростом количества онлайн-аккаунтов и подключенных к интернету устройств растут возможности злоумышленников, поэтому так важно знать правила безопасности в интернете – они помогут защититься от угроз и опасностей!

*Материалы подготовлены с использованием Интернет-ресурса «Лаборатория Касперского». -Режим доступа: https://www.kaspersky.ru

Основные рекомендации по безопасности в интернете

МБУ ДО «ДДТ» Дриада»

Пользователи интернета подвергаются целому ряду потенциальных угроз. Вот лишь основной список опасностей при использовании интернета:

- ⇒ **Кража идентификационных данных**
- ⇒ **Утечки данных**
- ⇒ **Вредоносные программы и вирусы**
- ⇒ **Фишинговые и мошеннические электронные письма**
- ⇒ **Поддельные сайты**
- ⇒ **Интернет-мошенничество**
- ⇒ **Мошенничество на сайтах и в приложениях для знакомств**
- ⇒ **Неприемлемый контент**
- ⇒ **Кибербуллинг**
- ⇒ **Неверные настройки конфиденциальности**

Чтобы избежать перечисленных опасностей, важно знать и соблюдать основные правила работы в интернете.

УБЕДИТЕСЬ, ЧТО ВАШЕ ИНТЕРНЕТ-СОЕДИНЕНИЕ ЗАЩИЩЕНО.

ИСПОЛЬЗУЙТЕ НАДЕЖНЫЕ ПАРОЛИ.

Надежный пароль обладает следующими свойствами:

- **Длинный: минимум 12 символов, в идеале, даже больше.**
- **Содержит заглавные и строчные буквы, а также специальные символы и цифры.**
- **Не очевидный: в пароле не используются комбинации последовательных цифр (1234) и личная информация, которую могут угадать (дата рождения или имя домашнего животного).**
- **Не содержит запоминающихся сочетаний клавиш.**

*Материалы подготовлены с использованием Интернет-ресурса «Лаборатория Касперского». -Режим доступа: https://www.kaspersky.ru

03 ПО ВОЗМОЖНОСТИ ВКЛЮЧИТЕ МНОГОФАКТОРНУЮ АУТЕНТИФИКАЦИЮ.

Многофакторная аутентификация – это способ проверки подлинности, при котором для доступа к учетной записи используются два или более метода проверки. Например, вместо простого запроса имени пользователя или пароля, при многофакторной аутентификации запрашивается дополнительная информация:

- **Дополнительный одноразовый пароль, который серверы аутентификации веб-сайта отправляют на телефон или электронную почту.**
- **Ответы на личные вопросы безопасности.**
- **Отпечаток пальца или другая биометрическая информация, например, голосовые данные или распознавание лица.**

04 ПОДДЕРЖИВАЙТЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ОПЕРАЦИОННЫЕ СИСТЕМЫ В АКТУАЛЬНОМ СОСТОЯНИИ.

Разработчики постоянно работают над безопасностью продуктов, отслеживая последние угрозы и выпуская исправления безопасности в случае обнаружения уязвимостей. Использование последних версий операционных систем и приложений позволяет применять последние исправления безопасности.

05 УБЕДИТЕСЬ, что ВЕБ-САЙТЫ ВЫГЛЯДЯТ и РАБОТАЮТ НАДЕЖНО.

Убедитесь, что веб-адрес сайта начинается с HTTPS, а не с HTTP (S означает «безопасный»), и что в адресной строке отображается значок замка.

Другие признаки надежности сайта включают:

- **Грамматически правильный текст без орфографических и пунктуационных ошибок. Качественные изображения, соответствующие ширине экрана.**
- **Объявления, органично вписанные в структуру сайта и не перегружающие его.**

*Материалы подготовлены с использованием Интернет-ресурса «Лаборатория Касперского». -Режим доступа: https://www.kaspersky.ru

СЛЕДИТЕ, ПО КАКИМ ССЫЛКАМ ВЫ ПЕРЕХОДИТЕ.

Один неосторожный переход по ссылке – и ваши личные данные попали к злоумышленникам или устройство заразилось вредоносной программой. Поэтому важно внимательно переходить по ссылкам и избегать определенных типов контента: ссылок из ненадежных источников, спам-сообщений, онлайн-викторин, кликбейтных заголовков, «бесплатных» предложений и нежелательной рекламы.

При получении электронного письма, в подлинности которого вы сомневаетесь, не переходите по содержащимся в нем ссылкам и не открывайте вложения.

Рекомендуется вообще не открывать такие сообщения. Если вы не уверены в подлинности электронного письма, обратитесь непосредственно к отправителю. Например, позвоните в банк и спросите, является ли полученное сообщение подлинным.

При просмотре сайта, убедитесь, что переход по ссылкам осуществляется на страницы со связанным или ожидаемым содержимым. Например, если вы переходите по ссылке, которая, как вам кажется, ведет на описание сафари в Африке, но вместо этого попадете на кликбейтную страницу о том, как похудели знаменитости или на статью с заголовком «Где они сейчас?», немедленно покиньте эту страницу.

ОБЕСПЕЧЬТЕ ЗАЩИТУ УСТРОЙСТВ.

Почти треть пользователей смартфонов не использует пароли, блокировку экрана и другие функции безопасности для защиты телефонов. Рекомендуется использовать пароли, секретные коды и другие средства безопасности, такие как считывание отпечатков пальцев или технологию распознавания лица на всех устройствах: телефонах, компьютерах, планшетах, умных часах, умных телевизорах и других устройствах.

РЕГУЛЯРНО ВЫПОЛНЯЙТЕ РЕЗЕРВНОЕ КОПИРОВАНИЕ.

Резервное копирование данных помогает минимизировать негативные последствия атак программ-вымогателей.

*Материалы подготовлены с использованием Интернет-ресурса «Лаборатория Касперского». -Режим доступа: https://www.kaspersky.ru

09 УДАЛЯЙТЕ НЕИСПОЛЬЗУЕМЫЕ УЧЕТНЫЕ ЗАПИСИ.

Слабые пароли, а сайты, на которых они использовались, могут иметь ненадежную политику защиты данных. Кроме того, по данным в старых профилях социальных сетей киберпреступники могут собрать о вас различные данные, например, дату рождения и местонахождение, и составить базовое представление.

10 БУДЬТЕ ОСТОРОЖНЫ С ЗАГРУЖЕННЫМИ ИЗ ИНТЕРНЕТА ОБЪЕКТАМИ.

Основная цель киберпреступников – обманным путем заставить пользователя загрузить вредоносные программы. Вредоносные программы могут быть замаскированы под различные приложения, от популярных игр до приложений для проверки трафика или погоды.

Вредоносные программы наносят ущерб: нарушают работу устройства, крадут личные данные, предоставляют несанкционированный доступ к компьютеру. Будьте осторожны при загрузке объектов на устройство, загружайте контент только из надежных или официальных источников.

11 БУДЬТЕ ОСТОРОЖНЫ С ИНФОРМАЦИЕЙ, ПУБЛИКУЕМОЙ В ИНТЕРНЕТЕ.

В интернете нет возможности удаления опубликованной информации. Все опубликованные комментарии и изображения могут навсегда остаться в сети, поскольку при удалении оригинала не происходит удаление копий, которые могли сделать другие пользователи.

Так же будьте осторожны, публикуя личную информацию в интернете: не указывайте адрес и дату рождения в биографических данных социальных сетей. В реальной жизни вы бы не сообщали личные данные незнакомцам, аналогично не следует публиковать их в интернете и делать доступными миллионам пользователей.

Соблюдайте осторожность при предоставлении адреса электронной почты. Полезно иметь дополнительную временную учетную запись электронной почты, используемую исключительно для регистрации и подписки. Она должна отличаться от рабочей и от используемой для переписки с друзьями и близкими.

*Материалы подготовлены с использованием Интернет-ресурса «Лаборатория Касперского». -Режим доступа: https://www.kaspersky.ru

12 ПЕРЕПРОВЕРЯЙТЕ НАЙДЕННУЮ В ИНТЕРНЕТЕ ИНФОРМАЦИЮ.

К сожалению, в интернете присутствует большое количество поддельных новостей и ложных сведений. В потоке получаемой ежедневно информации легко потеряться. Если вы сомневаетесь в достоверности прочитанной информации, проведите собственное исследование и установите реальные факты. На надежных веб-сайтах, как правило, приводятся ссылки на первоисточники, а на подозрительных страницах вообще не приведено никаких ссылок.

13 ИСПОЛЬЗУЙТЕ НАДЕЖНОЕ АНТИВИРУСНОЕ РЕШЕНИЕ и РЕГУЛЯРНО ОБНОВЛЯЙТЕ ЕГО

Помимо соблюдения рекомендаций по обеспечению безопасности в интернете, важно использовать надежное антивирусное решение. Программное обеспечение для безопасности в интернете защищает устройства и данные и блокирует не только распространенные угрозы, такие как вирусы и вредоносные программы, но и комплексные атаки с использованием приложений-шпионов, шифровальщиков и межсайтового скриптинга. Аналогично операционным системам и приложениям, также важно регулярно обновлять антивирус для защиты от новейших киберугроз.

14 ОЦЕНИТЕ И ОЗНАКОМТЕСЬ С ПАРАМЕТРАМИ И ПОЛИТИКАМИ КОНФИДЕНЦИАЛЬНОСТИ.

Многие из нас принимают политики конфиденциальности, не читая. Однако огромное количество данных обрабатывается в маркетинговых и рекламных целях, поэтому рекомендуется ознакомиться с политиками конфиденциальности используемых веб-сайтов и приложений и понять, как собираются и используются данные.

15 БУДЬТЕ ОСТОРОЖНЫ ПРИ ЗНАКОМСТВАХ В ИНТЕРНЕТЕ.

Ваши интернет-знакомые не всегда являются теми, за кого себя выдают. Они могут даже не являться реальными людьми. Используя поддельные профили в социальных сетях, злоумышленники охотятся за неосторожными пользователями с целью кражи их средств. К социальной жизни в интернете стоит относиться с такой же осторожностью, как и к социальной жизни в реальном мире.

*Материалы подготовлены с использованием Интернет-ресурса «Лаборатория Касперского». -Режим доступа: https://www.kaspersky.ru

ЭКСТРЕМИЗМ и ТЕРРОРИЗМ в сети Интернет

МБУ ДО «ДДТ» Дриада»

Большая часть преступлений, совершаемых с помощью Интернета, являются корыстными - кражи, мошенничества, вымогательство. Однако использование высоких технологий позволяет также готовить и осуществлять террористические акты, совершать экстремистские действия, несущие угрозу общественной безопасности, жизни и здоровью обычных граждан, где бы они ни находились, распространять и пропагандировать экстремистскую идеологию, вовлекая в противоправную деятельность новых членов.

Наряду с созданием и поддержанием собственных интернет-сайтов пропагандисты террора практикуют работу на форумах, в социальных сетях, порталах общего доступа.

Стоит отметить, что в последнее время в качестве платформы для совершения экстремистских преступлений с использованием сети Интернет все чаще используются такие мессенджеры, как Viber, WhatsApp и Telegram. Это связано в первую очередь с тем, что данные программы пользуются особыми методами шифрования сообщений, которые не поддаются отслеживанию и взлому.

Как выглядит экстремистский материал?

Конечно, признать тот или материал экстремистским может только суд, но знать и уметь находить признаки экстремизма должен уметь каждый. Итак, экстремистским является текст, видеоролик, аудиозапись, фотография, рисунок и т.п., если в них содержатся:

1) призывы к изменению государственного строя насильственным путем (т.е. призывы к революции, к восстанию, к неповиновению законно избранной власти, а также собственно эта деятельность);

2) призывы к осуществлению террористической деятельности или публичное оправдание терроризма, в том числе с использованием средств массовой информации (под этим понимается заявление того или иного лица (источника) о признании идеологии и практики терроризма правильными, нуждающимися в поддержке и подражании);

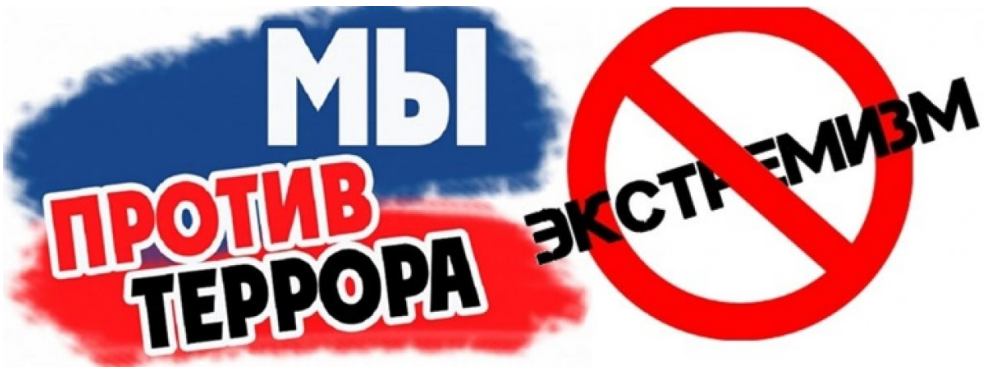
3) возбуждение социальной, расовой, национальной или религиозной розни (призывы к убийству, избиению или выселению лиц определенной национальности или вероисповедания);

4) пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности.

Если в увиденном вами материале присутствует хотя бы один из перечисленных признаков - относится к нему надо с повышенной настороженностью.

Опасность Интернет-экстремизма состоит в том, что он не имеет территориальных границ, поэтому деяния экстремистской направленности могут осуществляться из любой точки мира.

Как правило, обнаружить виновных в информационном пространстве сети Интернет очень сложно, так как они действует через один или несколько компьютеров с измененными (с помощью специального программного обеспечения) IP-адресами, что затрудняет их идентификацию и определение местоположения и обеспечивает высокую степень анонимности. Ряд сайтов экстремистских и взаимодействующих с ними террористических формирований создают сайты-«однодневки», меняют их форматы и адреса, что существенным образом затрудняет работу по их выявлению.



Как не попасть под влияние экстремистских и террористических организаций в сети Интернет?

В настоящее время все организации, действующие на территории России, в обязательном порядке проходят регистрацию в Министерстве юстиции РФ.

На сайте этого министерства в свободном доступе находится список таких организаций и также есть перечень организаций, признанных террористическими и экстремистскими, деятельность которых на территории Российской Федерации запрещена (эту информацию можно получить по ссылке http://www.fsb.ru/fsb/npd/terror.htm).

Если вы обнаружили, что вас заинтересовали материалы организации, включенной в список запрещенных на территории нашей страны, от посещения ее сайта, а тем более от контактов с ее представителями следует воздержаться. В противном случае вы, независимо от вашего собственного желания можете оказаться вовлечены в ее деятельность и рано или поздно будете привлечены к ответственности за свои противоправные поступки.

Не вступайте в переписку или видео-чат с незнакомыми вам людьми, особенно если они высказывают идеи экстремистского толка, с призывами к насильственным действиям, оскорблениями и унижениями по признакам расы, пола, национальности, религиозной принадлежности или атеистических убеждений и т.д.

Если все же такой диалог начался, попросите представиться вашего собеседника и спросите, какую организацию он представляет. При этом не исключено, что вас обманут и станут выдавать себя за другого. В такой ситуации продолжение взаимодействия недопустимо, даже если вы разделяете идеи собеседника или убеждены в своей правоте и стремитесь переубедить его. Опытному пропагандисту, прошедшему специальную подготовку, не составит большого труда навязать вам чуждые ценности и идеи, противостоять которым будет очень сложно.

Имейте в виду, что экстремистские и террористические группы националистического и религиозного толка нередко маскируются под «безобидные» общественные организации, деятельность которых на первых порах ограничивается заботой об охране окружающей среды, стремлением к здоровому образу жизни, сохранению семейных ценностей, проведению музыкальных и иных фестивалей и т.д., что само по себе никакой угрозы обществу не несет. Но на каком-то этапе они начинают проявлять свою истинную экстремистскую сущность, и в этом случае любой контакт с ним должен быть прекращен, какое бы психологическое давление они на вас ни оказывали.

В том случае, если вы чувствуете, что вам сложно самим принять такое решение, следует обратиться за помощью к людям, которым вы безусловно доверяете, или в соответствующие государственные органы власти.

Помните, что ваше участие в деятельности любой организации: политической, общественной, религиозной и т.п. - непосредственное (оффлайн) или в сети Интернет - это ваш личный выбор, и никто не вправе принуждать вас к такому участию.

Публичный призыв к экстремистской деятельности - это тяжкое преступление. Если призыв сделан в Интернете, то наказание за него - до 5 лет принудительных работ или лишения свободы.

При этом призыв необязательно должен иметь четкую грамматическую форму, соответствующую призыву, всякого рода намеки на необходимость сделать то-то и то-то тоже могут быть сочтены призывом.

Ни в коем случае не следует намекать на желательность (и тем более необходимость) переворота, сепаратизма, терроризма, возбуждения вражды к каким-то группам или их дискриминации, создания любых силовых помех органам власти, совершения любых преступлений по мотивам вражды к какой-то национальной, религиозной и т.п. группе, демонстрации запрещенной символики или финансирования всего перечисленного .