Аккредитованное образовательное частное учреждение
высшего образования
«Московский финансово-юридический университет
МФЮА» (МФЮА)

ПРИКАЗ

2 июля 2021 г. № 16-ро/169-3

Москва

Об утверждении локальных нормативных актов

В целях совершенствования локальной нормативной базы Аккредитованного образовательного частного учреждения высшего образования «Московский финансово-юридический университет МФЮА» и принимая во внимание Постановление Правительства РФ от 25.06.2021 N1019 «Об утверждении Положения о федеральном государственном контроле (надзоре) за соблюдением законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию»

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Правила использования на территории Аккредитованного образовательного частного учреждения высшего образования «Московский финансово-юридический университет МФЮА» и его филиалов персональных устройств несовершеннолетних обучающихся, имеющих возможность выхода в сеть «Интернет». (Приложение 1).

2. Утвердить и ввести в действие Положение об условиях присутствия обучающихся на публичном показе, при публичном исполнении, демонстрации посредством зрелищного мероприятия информационной продукции, запрещенной для детей, в случае их организации и (или) проведения в Аккредитованном образовательном частном учреждении высшего образования

«Московский финансово-юридический университет МФЮА» и в его филиалах. (Приложение 2).

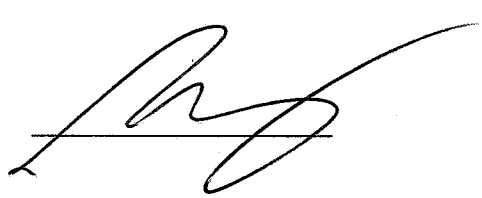
3. Утвердить и ввести в действие Положение о постоянно действующей комиссии по контролю за соблюдением законодательства о защите детей от информации, причиняющей вред их здоровью и развитию в Аккредитованном образовательном частном учреждении высшего образования «Московский финансово-юридический университет МФЮА». (Приложение 3).

4. Утвердить и ввести в действие Порядок рассмотрения обращения, жалоб или претензий о нарушении законодательства РФ о защите детей от информации, причиняющей вред их здоровью и развитию, включая несоответствие применяемых мер защиты детей от информации, запрещенной для распространения среди детей и направлении мотивированного ответа о результатах рассмотрения таких обращений, жалоб или претензий в Аккредитованном образовательном частном учреждении высшего образования "Московский финансово-юридический университет МФЮА". (Приложение 4).

5. Утвердить и ввести в действие Положение об обеспечении безопасности обучающихся во время пребывания в Аккредитованном образовательном частном учреждении высшего образования "Московский финансово-юридический университет МФЮА" и его филиалах. (Приложение 5).

6. Проректору по учебной работе Шутенко В.В. довести настоящий приказ до сведения руководителей структурных подразделений и обеспечить организацию размещения нормативного акта на сайте Университета не позднее 10 (десяти) рабочих дней после утверждения.

7. Контроль за исполнением данного приказа оставляю за собой.

Ректор  А.Г. Забелин

СОГЛАСОВАНО:

ДОЛЖНОСТЬ	***ПОДПИСЬ***	***ФИО***
Первый проректор		***О.А. Забелин***
Проректор по организационной работе		***О.А. Минаева***
Проректор по учебной работе		***В.В. Шутенко***
Председатель Студенческого совета		***В.В. Сладкова***

Приложение 1
к приказу МФЮА
от 2 июля 2021 г. № 16-10/169-3

УТВЕРЖДАЮ
Ректор МФЮА

(подпись)

А.Г. Забелин
(И.О. Фамилия)

ПРАВИЛА
использования на территории Аккредитованного образовательного частного учреждения высшего образования «Московский финансово-юридический университет МФЮА» и его филиалов персональных устройств несовершеннолетних обучающихся, имеющих возможность выхода в сеть «Интернет»

1. ЦЕЛИ И ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Правила использования на территории Аккредитованного образовательного частного учреждения высшего образования «Московский финансово-юридический университет МФЮА» и его филиалов персональных устройств несовершеннолетних обучающихся, имеющих возможность выхода в сеть «Интернет» (далее – Правила) определяют условия и порядок использования персональных устройств, имеющих возможность выхода в сеть «Интернет», в том числе средств мобильной связи (сотовые телефоны, смартфоны, планшеты) и других электронных устройств и гаджетов несовершеннолетними обучающимися в зданиях и на территории Аккредитованного образовательного частного учреждения высшего образования «Московский финансово-юридический университет МФЮА» и его филиалов (далее - Университет, МФЮА) во время образовательного процесса.

1.2. Правила разработаны в целях:

- повышения дисциплины участников образовательных отношений в ходе образовательной деятельности;

- уменьшения вредного воздействия радиочастотного и электромагнитного излучения средств мобильной связи и других электронных устройств на участников образовательного процесса;

- защиты обучающихся от информации, причиняющей вред их здоровью и развитию.

1.3. Настоящие Правила направлены на повышение качества и эффективности образовательной деятельности, обеспечение психологически комфортных условий образовательного процесса, защиту образовательного пространства МФЮА от информации, не связанной с образовательной деятельностью.

1.4. Требования настоящих Правил являются обязательными для структурных подразделений Университета, реализующих общеобразовательные программы, для остальных структурных

подразделений Университета, включая филиалы МФЮА, настоящие Правила носят рекомендательный характер.

2. ОСНОВНЫЕ ТЕРМИНЫ, СОКРАЩЕНИЯ

2.1. В настоящих Правилах используются следующие термины:

Гаджет (в настоящем документе) - устройство, присоединяемое к основного устройству и расширяющее его возможности.

Доступ обучающихся к информации - возможность получения и использования обучающимися свободно распространяемой информации.

Информационная безопасность обучающихся – состояние защищенности обучающихся, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

Информация, причиняющая вред здоровью и (или) развитию обучающихся – информация (в том числе содержащаяся в информационной продукции для обучающихся), распространение которой среди обучающихся запрещено или ограничено в соответствии с Федеральным законом от 29,12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

Пользователь - пользователь средств мобильной связи и других электронных устройств.

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1. Настоящие Правила разработаны в соответствии с:

– Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

– Федеральным законом от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;

– Методическими рекомендациями по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой

посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, утвержденными Министерством просвещения Российской Федерации, Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации, Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций 16.05.2019;

– Методическими рекомендациями об использовании устройств мобильной связи в общеобразовательных организациях, утвержденными Федеральной службой по надзору в сфере защиты прав потребителей и благополучия человека № МР 2.4.0150-19, Федеральной службой по надзору в сфере образования и науки № 01-230/13-01 14.08.2019 (вместе с «Результатами исследований, показавших отрицательные последствия использования устройств мобильной связи на здоровье детей»);

– Письмом Министерства образования и науки Российской Федерации от 14.05.2018 № 08-1184 «О направлении информации» (вместе с «Методическими рекомендациями о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети «Интернет»);

– Уставом МФЮА;

– Правилами внутреннего распорядка обучающихся в МФЮА;

– другими локальными нормативными актами МФЮА.

3.2. Настоящие Правила размещаются на официальном сайте МФЮА в разделе «Защита обучающихся от информации, причиняющей вред их здоровью и (или) развитию».

3.3. В МФЮА разработаны для несовершеннолетних обучающихся и их родителей (законных представителей) специальные памятки об информационной безопасности при использовании персональных устройств, имеющих возможность выхода в сеть «Интернет». Памятки размещаются на

официальном сайте МФЮА в разделе «Защита обучающихся от информации, причиняющей вред их здоровью и (или) развитию».

4. УСЛОВИЯ ИСПОЛЬЗОВАНИЯ СРЕДСТВ МОБИЛЬНОЙ СВЯЗИ И ДРУГИХ ЭЛЕКТРОННЫХ УСТРОЙСТВ

4.1. Использование средств мобильной связи во время образовательного процесса может нарушать права обучающихся на получение образования. Пользователи средств мобильной связи и других электронных устройств вправе использовать указанные средства, учитывая права и законные интересы окружающих лиц.

4.2. Во время учебных занятий обучающиеся могут пользоваться только теми техническими средствами, которые необходимы в образовательном процессе, или теми, которые разрешил использовать педагогический работник в образовательных целях.

4.3. До начала учебного занятия обучающиеся обязаны отключить или перевести средства мобильной связи и другие электронные устройства в режим «без звука», отключить режим вибрации во избежание возникновения фантомных вибраций, а также убрать их с рабочего стола.

4.4. Средства мобильной связи и другие электронные устройства, в том числе в выключенном состоянии, во избежание их порчи, потери и т.п. не должны находиться на рабочих столах в учебных аудиториях и на обеденных столах в столовой.

4.5. Использовать средства мобильной связи и другие электронные устройства разрешается до начала учебных занятий, после их окончания, на переменах.

4.6. Разрешение на аудио-, видеозапись учебного занятия/мероприятия, его фотосъемку дает лицо, проводящее мероприятие.

4.7. При пользовании средствами мобильной связи и другими электронными устройствами пользователи должны соблюдать этические нормы и правила поведения в общественных местах, в том числе:

– не устанавливать на средствах мобильной связи и других электронных устройствах громкие мелодии звонков и сообщений, мелодии и звуки, которые могут оскорбить или иным образом задеть окружающих; не вести приватные разговоры с использованием средств мобильной связи и других электронных устройств в присутствии других людей; разговаривать с собеседником максимально тихим голосом так, чтобы не мешать окружающим;

– не использовать чужие средства мобильной связи (электронные устройства) и не сообщать их номера третьим лицам без разрешения на то владельцев;

– не использовать средства мобильной связи и другие электронные устройства для ведения скрытой аудио-, видеозаписи, фотосъемки.

5. ПРАВА И ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ

5.1. Обучающиеся вправе использовать средства мобильной связи и другие электронные устройства вне учебных занятий или иных мероприятий, не нарушая права и законные интересы других участников образовательных отношений.

5.2. Несовершеннолетние обучающиеся для связи с родителями (законными представителями) во время учебного занятия в случае возникновения форс-мажорных обстоятельств вправе воспользоваться своим средством мобильной связи или иным электронным устройством с разрешения педагогического работника или представителя администрации Университета. Для связи с родителями (законными представителями) несовершеннолетний обучающийся должен выйти из учебной аудитории, чтобы не отвлекать педагогического работника и других обучающихся от учебного занятия.

После завершения разговора обучающийся обязан вернуться в учебную аудиторию, не отвлекая педагогического работника и других обучающихся.

5.3. Обучающимся запрещается использовать средство мобильной связи и другие электронные устройства на учебных занятиях в любом режиме (в том

числе как калькулятор, видеокамеру, диктофон и т. п.) кроме случаев, когда педагогический работник, проводящий занятие, разрешил такое использование в образовательных целях, а также за исключением обучающихся, нуждающихся в пользовании такими устройствами по состоянию здоровья (мониторинг сахара крови при сахарном диабете 1 типа и др.).

5.4. Обучающимся запрещается использовать средство мобильной связи и другие электронные устройства как средство получения информации из внешних источников, в том числе информации из Интернет и (или) социальных сетей, во время образовательного процесса, в том числе в целях поиска информации во время проведения проверочных, контрольных, лабораторных, практических и т.п. работ, кроме случаев, когда педагогический работник, проводящий занятие, разрешил такое использование в образовательных целях.

5.5. Регулярное использование обучающимся средств мобильной связи или иного электронного устройства во время образовательного процесса допускается при наличии исключительных причин по письменному разрешению руководителя учебного структурного подразделения МФЮА.

5.6. Родители (законные представители) несовершеннолетних обучающихся дают (или не дают) согласие о снятии ответственности с ректора МФЮА, руководителя учебного структурного подразделения МФЮА в случае предоставления своему ребенку данного устройства при посещении МФЮА, либо предоставляют согласие администрации МФЮА права на время учебного процесса забирать устройство(-а) несовершеннолетнего обучающегося.

5.7. Обучающиеся, пользователи средств мобильной связи и других электронных устройств вправе осуществлять фото- аудио- и видеосъемку лиц, находящихся в МФЮА исключительно с их согласия.

5.8. Сбор, хранение, использование и распространение информации, в том числе содержащей биометрические персональные данные допускается только при наличии согласия субъекта персональных данных.

5.9. На территории и в зданиях МФЮА запрещены демонстрация, публичный показ и распространение окружающим информационной продукции (аудиовизуальная продукция на любых видах носителей, информация, распространяемая посредством информационно-телекоммуникационных сетей, в том числе Интернет) ограниченной или запрещенной к распространению среди обучающихся. К такой информации, в частности относится фото-, видеоизображения, аудиозапись содержащие:

5.9.1. Информацию, побуждающую обучающихся к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству, либо жизни и (или) здоровью иных лиц, либо направленную на склонение или иное вовлечение обучающихся в совершение таких действий, а также содержащую экстремальные формы поведения: диггерство, руфинг, зацепинг, сталкерство, инфильтрация и т.п.

5.9.2. Информацию, способную вызвать у обучающихся желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством.

5.9.3. Информацию, обосновывающую или оправдывающую допустимость насилия и (или) жестокости либо побуждающую осуществлять насильственные действия по отношению к людям или животным.

5.9.4. Изображение или описание сексуального насилия.

5.9.5. Информацию отрицающую семейные ценности, пропагандирующую нетрадиционных сексуальных отношений и формирующую неуважение к родителям и (или) другим членам семьи.

5.9.6. Информацию оправдывающую противоправное поведение, содержащую нецензурную брань, информацию порнографического характера.

5.9.7. Информацию о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего.

5.10. В целях обеспечения сохранности средств мобильной связи и других электронных устройств пользователям не рекомендуется оставлять их без присмотра, в том числе в карманах верхней одежды в гардеробе.

6. ОТВЕТСТВЕННОСТЬ

6.1. Университет не несет ответственности за порчу или потерю средств мобильной связи и других электронных устройств, если их порча или потеря произошла по вине обучающегося в связи с нарушением настоящих Правил.

6.2. Обучающиеся МФЮА за нарушение настоящих Правил несут дисциплинарную ответственность в порядке, предусмотренном законодательством в сфере образования.

6.3. Родители (законные представители) несовершеннолетних обучающихся за порчу или потерю средства мобильной связи или другого электронного устройства своего ребенка, в связи с неисполнением им требований настоящих Правил и (или) технике безопасности, либо другого обучающегося учреждения, если порча или утеря вызвана нарушением настоящих Правил, дисциплины и т.п., несут материальную ответственность в порядке, предусмотренном гражданским законодательством.

Приложение №1

ИНФОРМАЦИОННАЯ ПАМЯТКА

для несовершеннолетних обучающихся

С каждым годом молодежи в интернете становится больше, а школьники одни из самых активных пользователей Рунета. Между тем, помимо огромного количества возможностей, интернет несет и проблемы. Эта памятка должна помочь безопасно находиться в сети.

Компьютерные вирусы

Компьютерный вирус — это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена зараженная программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

Методы защиты от вредоносных программ:

1. Используй современные операционные системы, имеющие серьезный уровень защиты от вредоносных программ;
2. Постоянно устанавливай патчи (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;
3. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
4. Ограничивай физический доступ к компьютеру для посторонних лиц;
5. Не открывай интернет-файлы, полученные из ненадежных источников. Далее те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Сети WI-FI

Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд «WECA», что обозначало словосочетание «Wireless Fidelity», который переводится как «беспроводная точность». До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура «Wi-Fi». Такое название было дано с намеком на стандарт высшей звуковой техники Hi-Fi, что в переводе означает «высокая точность».

Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.

Советы по безопасности работы в общедоступных сетях Wi-fi:

1. Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;
2. Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;
3. При использовании Wi-Fi отключи функцию «Общий доступ к файлам и

принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учебе;

4. Не используй публичный WI-FI для передачи личных данных, например, для выхода в социальные сети или в электронную почту;
5. Используй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно «https://»;
6. В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Социальные сети

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

Основные советы по безопасности в социальных сетях:

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;
3. Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;
4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее;
7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

Электронные деньги

Электронные деньги - это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.

Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах.

В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов - анонимные и не анонимные. Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в неанонимных идентификация пользователя является обязательной.

Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные нефиатные деньги (не равны государственным валютам).

Основные советы по безопасной работе с электронными деньгами:

1. Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства;

2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;

3. Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли - это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, $tR0ng!;;

4. Не вводи свои личные данные на сайтах, которым не доверяешь.

Электронная почта

Электронная почта - это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя пользователя@имя_домена. Также кроме передачи простого текста, имеется возможность передавать файлы.

Основные советы по безопасной работе с электронной почтой:

1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;
2. Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный_фанат@» или «рок2013» вместо «тема13»;
3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;
4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;
5. Если есть возможность написать самому свой личный вопрос, используй эту возможность;
6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;
7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;
8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».

Кибербуллинг или виртуальное издевательство

Кибербуллинг - преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Основные советы по борьбе с кибербуллингом:

1. Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;
2. Управляй своей киберрепутацией;

3. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;

4. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;

5. Соблюдай свою виртуальную честь смолоду;

6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;

7. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;

8. Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

Мобильный телефон

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений.

Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность.

Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-

то платные услуги; Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?

Необходимо обновлять операционную систему твоего смартфона; Используй антивирусные программы для мобильных телефонов;

Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;

После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies;

Периодически проверяй, какие платные услуги активированы на твоем номере; Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;

Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

Online игры

Современные онлайн-игры - это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции.

Все эти средства идут на поддержание и развитие игры, а также на саму безопасность: совершенствуются системы авторизации, выпускаются новые патчи (цифровые заплатки для программ), закрываются уязвимости серверов.

В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.

Основные советы по безопасности твоего игрового аккаунта:

1. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков;
2. Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов;

3. Не указывай личную информацию в профайле игры;

4. Уважай других участников по игре;

5. Не устанавливай неофициальные патчи и моды;

6. Используй сложные и разные пароли;

7. Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

Фишинг или кража личных данных

Обычной кражей денег и документов сегодня уже никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в интернет, и продолжают заниматься "любимым" делом.

Так появилась новая угроза: интернет-мошенничества или фишинг, главная цель которого состоит в получении конфиденциальных данных пользователей - логинов и паролей. На английском языке phishing читается как фишинг (от fishing - рыбная ловля, password - пароль).

Основные советы по борьбе с фитингом:

1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;

2. Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;

3. Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;

4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты; 5. Установи надежный пароль (PIN) на мобильный телефон;

6. Отключи сохранение пароля в браузере;

7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

Цифровая репутация

Цифровая репутация — это негативная или позитивная информация в сети о тебе. Компрометирующая информация, размещенная в интернете, может серьезным образом отразиться на твоей реальной жизни. "Цифровая репутация" — это твой имидж, который формируется из информации о тебе в интернете.

Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких — все это накапливается в сети.

Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу. Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающие люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой - как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

Основные советы по защите цифровой репутации:

1. Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;
2. В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только «для друзей»;
3. Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.

Авторское право

Современные обучающиеся - активные пользователи цифрового пространства. Однако далеко не все знают, что пользование многими возможностями цифрового мира требует соблюдения прав на интеллектуальную собственность.

Термин «интеллектуальная собственность» относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями.

Авторские права — это права на интеллектуальную собственность на произведения науки, литературы и искусства. Авторские права выступают в качестве гарантии того, что интеллектуальный/творческий труд автора не будет напрасным, даст ему справедливые возможности заработать на результатах своего труда, получить известность и признание. Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в Интернете. Использование «пиратского» программного обеспечения может привести ко многим рискам: от потери данных к твоим аккаунтам до блокировки твоего устройства, где установлена нелегальная программа. Не стоит также забывать, что существуют легальные и бесплатные программы, которые можно найти в сети.

Приложение №2

ПАМЯТКА

для родителей (законных представителей) несовершеннолетних обучающихся об информационной безопасности при использовании персональных устройств, имеющих возможность выхода в сеть «Интернет»

Определение термина «информационная безопасность детей» содержится в Федеральном законе от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (далее - Федеральный закон №436-ФЗ), регулирующим отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию. Согласно данному закону «информационная безопасность детей» - это состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

В силу Федерального закона № 436-ФЗ информацией, причиняющей вред здоровью и (или) развитию детей, является:

1. информация, запрещенная для распространения среди детей;
2. информация, распространение которой ограничено среди детей определенных возрастных категорий.

К информации, запрещенной для распространения среди детей, относится:

- информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в т.ч. причинению вреда своему здоровью, самоубийству;

- способность вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки,

изготавливаемые на его основе; принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

- обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям и животным;

- отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;

- оправдывающая противоправное поведение;

- содержащая нецензурную брань;

- содержащая информацию порнографического характера.

К информации, распространение которой ограничено среди детей определенного возраста, относится:

- информация, представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;

- 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;

- представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;

- содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

С учетом этого Вам предлагаются правила работы в сети Интернет для различных возрастных категорий, соблюдение которых позволит обеспечить информационную безопасность ваших детей.

Общие правила для родителей

1. Независимо от возраста ребенка используйте программное обеспечение, помогающее фильтровать и контролировать информацию, но не

полагайтесь полностью на него. Ваше внимание к ребенку - главный метод защиты.

2. Если Ваш ребенок имеет аккаунт на одном из социальных сервисов (LiveJournal, blogs.mail.ru, vkontakte.ru и т.п.), внимательно изучите, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео.

3. Проверьте, с какими другими сайтами связан социальный сервис Вашего ребенка. Странички Вашего ребенка могут быть безопасными, но могут и содержать ссылки на нежелательные и опасные сайты (например, порносайт, или сайт, на котором друг упоминает номер сотового телефона Вашего ребенка или Ваш домашний адрес)

4. Поощряйте Ваших детей сообщать обо всем странном или отталкивающем и не слишком остро реагируйте, когда они это делают (из-за опасения потерять доступ к Интернету дети не говорят родителям о проблемах, а также могут начать использовать Интернет вне дома и школы).

5. Будьте в курсе сетевой жизни Вашего ребенка. Интересуйтесь, кто их друзья в Интернет так же, как интересуетесь реальными друзьями.

Возраст детей от 13 до 17 лет

В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок «для взрослых». Девочки предпочитают общаться в чатах, при этом они гораздо более чувствительны к сексуальным домогательствам в Интернете.

Зачастую в данном возрасте родителям уже весьма сложно контролировать своих детей, так как об Интернете они уже знают значительно больше своих родителей. Тем не менее, не отпускайте детей в «свободное плавание» по Интернету. Старайтесь активно участвовать в общении ребенка в Интернете.

Важно по-прежнему строго соблюдать правила Интернет-безопасности - соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернете. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

Советы по безопасности в этом возрасте от 13 до 17 лет

1. Создайте список домашних правил посещения Интернета при участии подростков и требуйте безусловного его выполнения. Обговорите с ребенком список запрещенных сайтов («черный список»), часы работы в Интернете, руководство по общению в Интернете (в том числе в чатах).

2. Не забывайте беседовать с детьми об их друзьях в Интернете, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.

3. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

4. Необходимо знать, какими чатами пользуются Ваши дети. Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.

5. Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.

6. Приучите детей не выдавать свою личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.

7. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

8. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. 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.

9. Расскажите детям о порнографии в Интернете. Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

10. Приучите себя знакомиться с сайтами, которые посещают подростки.

11. Научите детей уважать других в интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде - даже в виртуальном мире.

12. Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

13. Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

14. Постоянно контролируйте использование Интернета Вашим ребенком! Это не нарушение его личного пространства, а мера предосторожности и проявление Вашей родительской ответственности и заботы.

Приложение №3

РАЗРЕШЕНИЕ
родителя (законного представителя) своему ребенку (несовершеннолетнему обучающемуся) пользоваться персональным устройством, имеющим возможность выхода в сеть «Интернет», при посещении МФЮА

Я, _____

фамилия, имя, отчество родителя (законного представителя)

являясь родителем (законным представителем) несовершеннолетнего обучающегося

_____

фамилия, имя, отчество обучающегося

кафедры _____

факультета _____

ознакомлен(а) с Перечнем видов информации, распространяемой посредствам сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования и порядком использования на территории МПГУ персональных устройств обучающихся, имеющих возможность выхода в сеть «Интернет», понимаю все правила и риски предоставления своему ребенку средств связи с выходом в сеть «Интернет».

Даю разрешение своему ребенку на пользование персональным мобильным средством при посещении МФЮА и снимаю ответственность с ректора МФЮА и руководителя учебного структурного подразделения за возможные последствия, в связи с предоставлением своему ребенку такого права.

_____

(ФИО, дата, подпись)

**Разрешение подписывают родители всех обучающихся, независимо от того имеется или не имеется на момент подписания согласия у ребенка устройство с выхода в сеть «Интернет», т.к. согласие действует со дня его подписания на весь период обучения ребенка.*

Приложение №4

СОГЛАСИЕ

родителя (законного представителя) несовершеннолетнего обучающегося на предоставление права администрации МФЮА изымать на время нахождения такого обучающегося на территории МФЮА у него любое персональное устройство, имеющее возможность выхода в сеть «Интернет»

Я, _____

фамилия, имя, отчество родителя (законного представителя)

являясь родителем (законным представителем) несовершеннолетнего обучающегося

_____

фамилия, имя, отчество обучающегося

кафедры _____

факультета _____

ознакомлен(а) с Перечнем видов информации, распространяемой посредствам сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования и порядком использования на территории МФЮА персональных устройств обучающихся, имеющих возможность выхода в сеть «Интернет», предоставляю право администрации МФЮА изымать на время нахождения моего ребенка на территории МФЮА у него любое персональное устройство, имеющее возможность выхода в сеть «Интернет».

_____

(ФИО, дата, подпись)