«УТВЕРЖДАЮ»
Директор ГБПОУ «КОР ПК»
С.Ю. Гончарова
«30» декабря 2020 г.

ПОЛОЖЕНИЕ
об информационной безопасности и мониторинге социальных сетей в ГБПОУ «Колледж олимпийского резерва Пермского края»

УД-01.02.29 - 20

	Должность	*Фамилия*	*Подпись*
Разработал	*Директор*	*С.Ю. Гончарова*	
Проверил			
Согласовано			
Версия: 1.0	*Без подписи документ действителен 8 часов после распечатки.*		Стр. 7

Приложение 1 к приказу от 30.12.2020 г. № 211/од

1. Общие положения

1.1. Настоящее Положение об информационной безопасности и мониторинге социальных сетей в ГБПОУ «Колледж олимпийского резерва Пермского края» (далее – Положение, Учреждение) предусматривает принятие необходимых мер в целях защиты данных от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в Учреждении, а также соблюдения законодательства в области профилактики безнадзорности и правонарушений несовершеннолетних.

1.2. Ответственность за соблюдение информационной безопасности несет каждый работник Учреждения, в том числе работающий по совместительству.

Ответственность за проведение мониторинга социальных сетей с целью выявления несовершеннолетних, состоящих в группах деструктивной направленности несут руководители учебных групп.

1.3. Целями настоящего Положения являются:

сохранение конфиденциальности информационных ресурсов;

обеспечение непрерывности доступа к информационным ресурсам Учреждения для поддержки деятельности;

защита целостности деловой информации с целью поддержания возможности Учреждения по оказанию услуг высокого качества и принятию эффективных управленческих решений;

повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами Учреждения;

определение степени ответственности и обязанностей работников по обеспечению информационной безопасности в Учреждении;

выявление несовершеннолетних, состоящих в группах деструктивной направленности, и организация профилактической работы с ними и их семьями.

1.4. Заместители директора по направлениям деятельности должны обеспечивать регулярный контроль за соблюдением Положения.

1.5. Системным администратором колледжа организуется периодическая проверка соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки директору Учреждения.

1.6. Требования настоящего Положения распространяются на всю информацию и ресурсы обработки информации Учреждения.

2. Основные требования информационной безопасности

2.1. Ответственность за информационные активы и контроль доступа к информационным системам

В отношении всех информационных активов Учреждения, активов, находящихся под контролем Учреждения, а также активов, используемых для получения доступа к инфраструктуре Учреждения, определена ответственность соответствующих работников Учреждения.

Все работы в пределах Учреждения выполняются в соответствии с должностными обязанностями только на компьютерах, разрешенных к использованию в Учреждении.

Допускается использование в здании и помещениях Учреждения личных портативных компьютеров и внешних носителей информации (диски, дискеты, флэш-карты и т.п.) без возможности подключения к локальной сети Учреждения.

Для использования общих сетевых ресурсов пользователи обязаны вводить логин и пароль при каждом подключении к сетевому ресурсу.

Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Запрещается сообщать свой пароль другим

лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким, если работа выполняется дома.

В процессе своей работы сотрудники обязаны постоянно использовать режим "Экранной заставки" с парольной защитой. Рекомендуется устанавливать максимальное время "простоя" компьютера до появления экранной заставки не дольше 15 минут.

2.2. Доступ третьих лиц к системам Учреждения

Каждый сотрудник обязан немедленно уведомить руководство или системного администратора обо всех случаях предоставления доступа третьим лицам к ресурсам сети Учреждения.

Доступ третьих лиц к информационным системам Учреждения должен быть обусловлен производственной необходимостью. В связи с этим, порядок доступа к информационным ресурсам Учреждения должен быть четко определен, контролируем и защищен.

Не допускается доступ студентов колледжа к рабочим местам сотрудников, предназначенных для служебного пользования и подключенных к локальной сети Учреждения.

2.3. Удаленный доступ

Пользователи получают право удаленного доступа к информационным ресурсам Учреждения с учетом их взаимоотношений с Учреждением.

Сотрудникам, использующим в работе портативные компьютеры Учреждения, может быть предоставлен удаленный доступ к сетевым ресурсам Учреждения в соответствии с правилами информационной системы Учреждения.

Сотрудникам, работающим за пределами Учреждения с использованием компьютера, не принадлежащего Учреждению, запрещено копирование данных на компьютер, с которого осуществляется удаленный доступ.

Сотрудники и третьи лица, имеющие право удаленного доступа к информационным ресурсам Учреждения, должны соблюдать требование, исключающее одновременное подключение их компьютера к сети Учреждения и к каким-либо другим сетям, не используемые Учреждением.

Все компьютеры, подключаемые посредством удаленного доступа к информационной сети Учреждения, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

2.4. Доступ к сети Интернет

Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.

Сотрудникам Учреждения:

разрешается использовать сеть Интернет только в служебных целях;

запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности;

запрещается использовать сеть Интернет для хранения данных Учреждения;

разрешается использовать Интернет-ресурсы только режимом просмотра информации, исключая возможность передачи информации Учреждения в сеть Интернет;

перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;

запрещается посещение и использование социальных сетей.

Руководство учреждения и системный администратор имеют право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

2.5. Защита оборудования

Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранятся информация Учреждения.

Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения может производить только системный администратор, либо специалисты, имеющие определенный допуск к аппаратному и программному обеспечению.

Любые изменения в конфигурации аппаратного и программного обеспечения осуществляются только после согласования с руководством Учреждения.

2.6. Аппаратное и программное обеспечение

Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (принтеры и сканеры), аксессуары (манипуляторы типа «мышь», шаровые манипуляторы, дисководы для CD-дисков), коммуникационное оборудование (факс-модемы, сетевые адаптеры и концентраторы), предоставленное Учреждением, является его собственностью и предназначено для использования исключительно в производственных целях.

Пользователи портативных компьютеров, содержащих информацию, составляющую коммерческую тайну Учреждения, обязаны обеспечить их хранение в физически защищенных помещениях, запираемых ящиках рабочего стола, шкафах, или обеспечить их защиту с помощью аналогичного по степени эффективности защитного устройства, в случаях, когда данный компьютер не используется.

Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности, как на работе, так и по месту проживания.

Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов.

Все программное обеспечение, установленное на предоставленном Учреждения компьютерном оборудовании, является собственностью Учреждения и должно использоваться исключительно в производственных целях.

Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности. Если в ходе выполнения технического обслуживания будет обнаружено не разрешенное к установке программное обеспечение, оно будет удалено, а сообщение о нарушении будет направлено руководству Учреждения.

На всех портативных компьютерах, принадлежащих Учреждению, должно быть установлено антивирусное программное обеспечение.

Все компьютеры, подключенные к корпоративной сети, должны быть оснащены системой антивирусной защиты.

Сотрудники Учреждения не должны:

блокировать антивирусное программное обеспечение;

устанавливать другое антивирусное программное обеспечение;

изменять настройки и конфигурацию антивирусного программного обеспечения.

2.7. Обязанности специалиста по информационной безопасности (системного администратора):

Выполняет мероприятия по обеспечению безопасности информации в ключевых системах информационной инфраструктуры.

Определяет возможные угрозы безопасности информации, уязвимость программного и аппаратного обеспечения, разрабатывает технологии обнаружения вторжения, оценивает и переоценивает риски, связанные с угрозами деструктивных информационных воздействий, способных нанести ущерб системам и сетям вследствие несанкционированного доступа, использования раскрытия, модификации или уничтожения информации и ресурсов информационно-управляющих систем.

Определяет ограничения по вводу информации, процедуры управления инцидентами нарушения безопасности и предотвращает их развитие, порядок подключения к открытым информационным системам с учетом обеспечения безопасности, связанной с соглашениями о доступе и приоритезации ресурсов, требования к местам резервного хранения, обработки и копирования информации, приоритеты обслуживания по использованию основных и резервных

телекоммуникационных сервисов (услуг).

Разрабатывает процедуры защиты носителей информации, коммуникаций и восстановления информационно-управляющих систем после сбоя или отказа.

Осуществляет контроль деятельности по обеспечению безопасности информации в ключевых системах информационной инфраструктуры; информационное, материально-техническое и научно-техническое обеспечение безопасности информации; контроль состояния работ по обеспечению безопасности информации в ключевых системах информационной инфраструктуры и их соответствие нормативным правовым актам Российской Федерации.

Дает отзывы и заключения на проекты вновь создаваемых и модернизируемых объектов и других разработок по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры.

Участвует в рассмотрении технических заданий на научно-исследовательские и опытно-конструкторские работы по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, оценивает их соответствие действующим нормативным и методическим документам.

Участвует в работах по внедрению новых средств технической защиты информации.

Содействует распространению в Учреждении передового опыта и внедрению современных организационно-технических мер, средств и способов обеспечения безопасности информации в ключевых системах информационной инфраструктуры.

Проводит оценки технико-экономического уровня и эффективности предлагаемых и реализуемых организационно-технических решений по обеспечению безопасности информации в ключевых системах информационной инфраструктуры.

Участвует в разработке списков доступа персонала на объекты защиты, порядок и правила поведения работников, в том числе при их перемещении, увольнении и взаимодействии с персоналом сторонних организаций.

3. Правила пользования электронной почтой

Содержание электронных сообщений должно строго соответствовать стандартам Учреждения в области деловой этики.

Использование электронной почты в личных целях допускается в случаях, когда получение/отправка сообщения не мешает работе других пользователей и не препятствует деятельности.

Сотрудникам Учреждения запрещается использовать публичные почтовые ящики электронной почты или персональные почтовые ящики для осуществления какого-либо из видов корпоративной деятельности.

Использование сотрудниками Учреждения публичных и персональных почтовых ящиков электронной почты осуществляется только при согласовании с руководством Учреждения.

Сотрудники Учреждения для обмена документами с другими учреждениями должны использовать только официальный адрес электронной почты.

Сообщения, пересылаемые по электронной почте, представляют собой постоянно используемый инструмент для электронных коммуникаций, имеющих тот же статус, что и письма и факсимильные сообщения. Электронные сообщения подлежат такому же утверждению и хранению, что и прочие средства письменных коммуникаций.

В целях предотвращения ошибок при отправке сообщений пользователи перед отправкой должны внимательно проверить правильность написания имен и адресов получателей. В случае получения сообщения лицом, вниманию которого это сообщение не предназначается, такое сообщение необходимо переправить непосредственному получателю.

Отправитель электронного сообщения, документа или лицо, которое его переадресовывает, должен указать свое имя и фамилию, служебный адрес и тему сообщения.

Недопустимые действия сотрудников:

рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;

рассылка рекламных материалов, не связанных с деятельностью Учреждения;

подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;

поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);

пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, которое может рассматриваться как уголовное преступление или административный проступок либо приводит к возникновению гражданско-правовой ответственности, беспорядков или противоречит корпоративным стандартам в области этики.

Ко всем исходящим сообщениям, направляемым внешним пользователям, пользователь может добавлять уведомление о конфиденциальности.

Вложения, отправляемые вместе с сообщениями, следует использовать с должной осторожностью. Во вложениях всегда должна указываться дата их подготовки, и они должны оформляться в соответствии с установленными в Учреждении процедурами документооборота.

4. Сообщение об инцидентах информационной безопасности, реагирование и отчетность

Все пользователи должны сообщать об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

В случае кражи переносного компьютера следует незамедлительно сообщить об инциденте руководству Учреждения.

Пользователи должны знать способы информирования об известных или предполагаемых случаях нарушения информационной безопасности с использованием телефонной связи, электронной почты и других методов. Необходимо обеспечить контроль и учет сообщений об инцидентах и принятие соответствующих мер.

Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:

проинформировать системного администратора;

не пользоваться и не выключать зараженный компьютер;

не подсоединять этот компьютер к компьютерной сети Учреждения до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование системным администратором.

5. Управление сетью

5.1. Уполномоченные сотрудники контролируют содержание всех потоков данных проходящих через сеть Учреждения.

Сотрудникам Учреждения запрещается:

нарушать информационную безопасность и работу сети Учреждения;

сканировать порты или систему безопасности;

контролировать работу сети с перехватом данных;

получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;

использовать любые программы, скрипты, команды или передавать сообщения с целью вмешаться в работу или отключить пользователя оконечного устройства;

передавать информацию о студентах и сотрудниках Учреждения посторонним лицам;

создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

5.2. Защита и сохранность данных

Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях.

Необходимо регулярно делать резервные копии всех основных служебных данных и программного обеспечения.

Только системный администратор на основании заявок руководителей подразделений может создавать и удалять совместно используемые сетевые ресурсы и папки общего пользования, а также управлять полномочиями доступа к ним.

Сотрудники имеют право создавать, модифицировать и удалять файлы и директории в совместно используемых сетевых ресурсах только на тех участках, которые выделены лично для них, для их рабочих групп или к которым они имеют санкционированный доступ.

5.3. Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть документированы, согласованны с руководителями Учреждения и системным администратором.

6. Мониторинг социальных сетей социальных сетей с целью выявления несовершеннолетних, состоящих в группах деструктивной направленности

6.1. Задачи мониторинга социальных сетей несовершеннолетних обучающихся:

определение круга пользователей социальными сетями из числа обучающихся ГБПОУ «Колледж олимпийского резерва Пермского края»;

выявление признаков девиантного поведения пользователей, указанной категории;

выявление фактов распространения информации, склоняющей несовершеннолетних к асоциальному поведению;

своевременное выявление информации, причиняющей вред их здоровью и развитию (пропаганда суицидов, порнография, пропаганда насилия, экстремизм, агрессия, кибербуллинг, киднеппинг и т.д.).

6.2. К действиям руководителей учебных групп по подготовке и проведению мониторинга социальных сетей относится:

проверка страницы при помощи программы Герда Бот;

анализ страницы пользователя (профиля) социальной сети;

анализ терминологии и маркеров, используемых на странице;

анализ содержания фото, аудио и видеоматериалов, выложенных на странице;

соблюдение конфиденциальности.

6.3. Отчет о результатах мониторинга предоставляется ежемесячно до 5-го числа месяца, следующего за отчетным периодом (Приложение 1).

6.4. Результаты мониторинга следует учитывать при разработке и корректировке планов воспитательной работы, планов индивидуально-профилактической работы, планировании мероприятий, организации работы с активом обучающихся.

6.5. В случае выявления информации, причиняющей угрозу жизни обучающемуся, следует:

незамедлительно передать информацию, вышестоящим органам (ответственному за социальной работу, заведующему отделением, заместителю директора, директору);

незамедлительно передать информацию в комиссию по делам несовершеннолетних и защите прав ребенка (Приложение 2);

составить план по устранению фактов принадлежности обучающегося к деструктивным группам.

Приложение 1

Мониторинг социальных сетей

Отчет куратора группы за _____ месяц 202_____ года

Проверено _____ аккаунтов студентов группы _____

Проверка осуществлялась при помощи программы Герда бот и методом педагогического наблюдения и анализа странички в сети ВКонтакте (др.).

Результат (для примера):

материалы, размещенные на странице несовершеннолетних, проверены с помощью программы Герда бот – запрещенные материалы и группы не выявлены.

Среди фото-, видео- и аудио материалов, размещенных на страницах студентов, подозрительных обнаружено не было.

В случае выявления фактов принадлежности к деструктивным группа заполняется таблица

ФИО несовершеннолетнего, дата рождения	Категория учета (норма, группа риска СОП, СОП)	Ник в сети	Адрес страницы в сети ВКонтакте	Отметка о состоянии деструктивных и асоциальных группах в социальной сети

Дата _____

Руководитель учебной группы _____

Приложение 2

Информация о выявленных фактах
(для направления в КДНиЗП)

№ п/п	ФИО обучающегося, дата рождения	Категория учета (норма, группа риска СОП, СОП)	Ник в сети	Адрес страницы в сети ВКонтакте	Отметка о состоянии деструктивных и асоциальных группах в соцсети