НОУ ДПО УМЦ
НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
УЧЕБНО-МЕТОДИЧЕСКИЙ ЦЕНТР

Фактический адрес: 650000, Российская Федерация, г. Кемерово, ул. Шестакова, 6
Почтовый адрес: 650000, Российская Федерация, г. Кемерово, пр. Кузнецкий, 17, оф. 206
Телефон/факс: 8(3842) 45-41-11, 36-56-05, 36-58-12, E-mail: umc.pk@mail.ru Web: www.umc-kem.ru
ОКПО 85223316, ОГРН 1084200002260, ИНН/КПП 4205152080/420501001

УТВЕРЖДАЮ
Директор НОУ ДПО «УМЦ»

_____ Е.П. Лодза
«02» 06 2017 г.

Выпуск № 1

Дата введения в действие 01.06.2017 г.

Введено в действие приказом № ____от 01.06.2017 г.

ПОЛОЖЕНИЕ
Об информационной безопасности

	Разработал	Согласование		
Должность	Руководитель информационно – аналитической группы отдела перспективного развития	Начальник отдела перспективного развития	Начальник отдела по работе с персоналом	Юрисконсульт
ФИО	Кузьмин Алексей Олегович	Лодза Даниил Евгеньевич	Токарева Алена Сергеевна	Арышева Алена Игоревна
Дата	26.05.2017г	26.05.2017г	26.05.2017	26.05.2017г
Подпись				

Кемерово, 2017 г.

1. ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1 Настоящее Положение определяет цель, принципы и основные направления защиты информации в компьютерной сети НОУ ДПО «УМЦ» (далее Учреждение), порядок эксплуатации объектов информатизации Учреждения, регламентация взаимодействия подразделений Учреждения в процессе управления информацией, формируемой с использованием средств вычислительной техники, определение условий эксплуатации информационно–вычислительных систем Учреждения, предотвращение нарушения конфиденциальности и сохранности данных.

1.2 Действие настоящего положения распространяется на все структурные подразделения Учреждения.

1.3 Ответственность за поддержание актуальности, своевременный пересмотр и контроль за соблюдением требований данного положения несет начальник отдела перспективного развития (далее по тексту **ОПР**) и руководитель информационно – аналитической группы отдела перспективного развития (далее по тексту **ИАГ ОПР**).

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1 **Сервер** – аппаратно–программный комплекс, исполняющий функции хранения и обработки запросов пользователей и не предназначенный для локального доступа пользователей (выделенный сервер, маршрутизатор и другие специализированные устройства) ввиду высоких требований по обеспечению надежности, степени готовности и мер безопасности информационной системы предприятия.

2.2 **Рабочая станция** – персональный компьютер (терминал), предназначенный для доступа пользователей к ресурсам Автоматизированной системы предприятия, приема передачи и обработки информации.

2.3 **Автоматизированная система** – совокупность программных и аппаратных средств, предназначенных для хранения, передачи и обработки данных и информации, и производства вычислений.

2.4 **Системный администратор** – должностное лицо (сотрудник **ИАГ ОПР**), в обязанности которого входит обслуживание всего аппаратно–программного комплекса Учреждения, управление доступом к сетевым ресурсам, а также поддержание требуемого уровня отказоустойчивости и безопасности данных, их резервное копирование и восстановление.

2.5 **Пользователь** – сотрудник Учреждения, использующий ресурсы автоматизированной информационной системы предприятия для выполнения должностных обязанностей.

2.6 **Служебные группы безопасности и почтовой рассылки** – объекты безопасности, необходимые для управления доступом к служебному программному обеспечению и рассылки уведомлений, предназначенных персоналу информационно – аналитической группы.

2.7 **Пароль:** – секретная строка символов (букв, цифр, специальных символов), предъявляемая пользователем компьютерной системе для получения доступа к данным и программам. Пароль является средством защиты данных от несанкционированного доступа.

2.8 **Первичный пароль** – комбинация символов (буквы, цифры, знаки препинания, специальные символы), устанавливаемые системным администратором при создании новой учетной записи.

2.9 **Основной пароль** – комбинация символов (буквы, цифры, знаки препинания, специальные символы), известная только сотруднику организации, используемая для подтверждения подлинности владельца учетной записи.

2.10 **Административный пароль** – комбинация символов (буквы, цифры, знаки препинания, специальные символы), известная системному администратору, руководителю информационно – аналитической группы),

используемая при настройке служебных учетных записей, учетных записей служб и сервисов, а также специальных учетных записей.

2.11 **Изменение полномочий** – процесс создания, удаления, внесения изменений в учетные записи пользователей автоматизированной системы, создание, удаление изменение наименований почтовых ящиков и адресов электронной почты, создание, удаление изменение групп безопасности и групп почтовой рассылки, а также другие изменения, приводящие к расширению (сокращению) объема информации либо ресурсов доступных пользователю автоматизированной системы.

2.12 **Учетная запись** – информация о сетевом пользователе: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе в системе. Учетная запись может содержать дополнительную информацию (Адрес электронной почты, телефон и т.п.).

2.13 **Служебная учетная запись** – объекты безопасности, содержащие реквизиты, необходимые для нормального функционирования некоторых служб и сервисов (например, задачи резервного копирования и восстановления, служба автоматического обновления операционной системы и т.п.).

2.14 **Локальные учетные записи** – это учетные записи, созданные операционной системой во время ее установки и хранящиеся на локальном компьютере.

2.15 **Специальные учетные записи** – реквизиты доступа к активному сетевому оборудованию, учетные записи для доступа к базам данным, а также все учетные записи, реквизиты которых не хранятся в едином каталоге AD.

2.16 **Служебная информация** – это информация, полученная путем ведения трудовой деятельности сотрудников НОУ ДПО «УМЦ».

2.17 **Сетевая папка** – информационный ресурс, расположенный удаленно на выделенном сервере или специализированной системе хранения данных.

2.18 **Антивирусное средство** – специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1 Организационное и техническое обеспечение рабочего процесса сотрудников Учреждения возлагается на сотрудников **ИАГ ОПР**.

3.2 С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику Учреждения, допущенному к работе с конкретной подсистемой автоматизированной системы, должно быть сопоставлено персональное уникальное имя – учетная запись пользователя и пароль, под которым он будет регистрироваться, и работать в системе. Использование несколькими сотрудниками при работе в автоматизированной системе одного и того же имени пользователя **ЗАПРЕЩЕНО**.

3.3 Основанием для изменения полномочий (предоставления, изменения либо прекращения действий прав доступа пользователя автоматизированной системы) является письменная заявка сотрудника (**Приложение №1**), для которого требуется изменить полномочия доступа к системе на имя Директора Учреждения, которая после утверждения направляется начальнику **ОПР**, или исполняющему обязанности начальнику **ОПР**, при его отсутствии.

3.4 Проведение операций, указанных п.2.11 сотрудниками **ИАГ ОПР**, не уполномоченными на проведение подобных действий – **ЗАПРЕЩЕНО** и идентифицируется как факт несанкционированного доступа.

3.5 С целью выявления фактов и предотвращения несанкционированного доступа, контроля доступа к автоматизированным системам применяются специализированные программные комплексы, утвержденные Директором

Учреждения в списке разрешенного программного обеспечения или аппаратные средства (дополнительное оборудование).

4. ПОРЯДОК СОЗДАНИЯ, ИЗМЕНЕНИЯ И УДАЛЕНИЯ УЧЕТНЫХ ЗАПИСЕЙ, ГРУПП БЕЗОПАСНОСТИ И ПОЧТОВОЙ РАССЫЛКИ

4.1 Первичная заявка «На внесение изменений в списки пользователей автоматизированной системы и наделения пользователей полномочиями доступа к ресурсам» (далее по тексту – **ЗАЯВКА**) (**Приложение №1**), оформляется при приеме на работу в отделе по работе с персоналом за подписью руководителя структурного подразделения по направлению деятельности.

4.2 Инициатор изменения либо удаления созданных учетных записей повторно оформляет **ЗАЯВКУ**.

4.3 **ЗАЯВКУ** утверждает директор НОУ ДПО «УМЦ».

4.4 Утвержденная **ЗАЯВКА** поступает в **ОПР**.

4.5 **ЗАЯВКА** должна быть обработана и исполнена системным администратором в течении рабочего дня с момента получения.

4.6 Проведение изменений, указанных п.2.11 системным администратором без наличия **ЗАЯВКИ** «На внесение изменений в списки пользователей» категорически **ЗАПРЕЩЕНО**.

4.7 **Изменение полномочий учетных записей и состава групп безопасности и почтовой рассылки:**

4.7.1 Системный администратор вносит соответствующие изменения в базу данных учетных записей.

4.8 **Создание новых учетных записей пользователей групп безопасности и почтовой рассылки:**

4.8.1 Системный администратор создает необходимые объекты безопасности, присваивает первичный пароль вновь созданной учетной записи, при необходимости создает почтовый ящик пользователя.

4.8.2 При задании первичного пароля учетной записи пользователя системный администратор обязан установить отметку «Потребовать смену пароля при первом входе в систему» Допускается в качестве первичного пароля использовать простые или повторяющиеся комбинации.

4.8.3 После выполнения системный администратор передает бланк **ЗАЯВКИ**, а также дополнительную информацию необходимую для использования вновь созданного объекта безопасности (первичный пароль, «имя» учетной записи адрес электронной почты и т.п.) начальнику **ОПР**.

4.9 **Удаление учетных записей пользователей групп безопасности и почтовой рассылки:**

4.9.1 Системный администратор удаляет необходимые объекты безопасности из всех указанных списков доступа.

4.9.2 После выполнения изменений системный администратор передает **ЗАЯВКУ** руководителю **ИАГ ОПР**.

4.10 Исполненная **ЗАЯВКА** остается на хранении в **ИАГ ОПР**.

4.11 Копия исполненной **ЗАЯВКИ** передается инициатору.

5. СЛУЖЕБНЫЕ УЧЕТНЫЕ ЗАПИСИ И ГРУППЫ

5.1 Служебные учетные записи **НЕ ПРЕДНАЗНАЧЕНЫ** для локального входа в систему, работа сотрудников **ИАГ ОПР** с использованием реквизитов служебных учетных записей – **ЗАПРЕЩЕНА**.

5.2 Создание удаление и изменение служебных объектов безопасности производятся системным администратором по письменной или электронной заявке начальника **ОПР**.

5.3 Самостоятельное создание, изменение либо удаление служебных учетных записей системным администратором – **ЗАПРЕЩЕНО**.

5.4 Категорически запрещается использование встроенной учетной записей **Administrator** (**Администратор**) (**SA** для SQL сервера и т.п.) – для повседневной работы, для запуска служб и сервисов либо для доступа к сетевым ресурсам. Использование встроенных учетных записей допускается только в случаях, требующих реквизитов именно этой учетной записи (восстановление AD, восстановление поврежденных данных системы, в некоторых случаях проведение обновлений системы и т.п.).

5.5 Решение о необходимости применения реквизитов служебных учетных записей принимает системный администратор.

6. ЛОКАЛЬНЫЕ УЧЕТНЫЕ ЗАПИСИ

6.1 Локальные учетные записи (Administrator, Guest) предназначены для служебного использования системными администраторами при настройке системы и не предназначены для повседневной работы.

6.2 Создание и использование локальных учетных записей на рабочих станциях – **ЗАПРЕЩЕНО**.

6.3 Встроенная учетная запись Guest (Гость) должна быть заблокирована на всех рабочих станциях при первоначальном конфигурировании операционной системы.

7. СПЕЦИАЛЬНЫЕ УЧЕТНЫЕ ЗАПИСИ

7.1 Создание специальных учетных записей производится системным администратором при возникновении необходимости по согласованию с начальников **ОПР**.

7.2 Утвержденный директором Учреждение список специальных учетных записей храниться у руководителя **ИАГ ОПР.**

8. ТРЕБОВАНИЯ К ПАРОЛЯМ

8.1 Установку первичного пароля производит системный администратор при создании новой учетной записи.

8.2 Первичный пароль может содержать несложную комбинацию символов, либо повторяющиеся символы.

8.3 При создании первичного пароля, системный администратор обязан установить опцию, «Требовать смены пароля при следующем входе в систему», а также уведомить владельца учетной записи о необходимости произвести смену пароля.

8.4 Первичный пароль так же используется при сбросе забытого пароля на учетную запись. В любом случае, при использовании первичного пароля все требования настоящего документа сохраняются.

8.5 Установку основного пароля производит пользователь при первом входе в систему с новой учетной записью.

8.6 При выборе пароля необходимо руководствоваться следующими правилами:

- Длинна пароля, должна составлять не менее 8 символов;
- При выборе пароля, рекомендуется использовать комбинацию из строчных и прописных букв, цифр, знаков препинания и специальных символов;
- Запрещается использовать в качестве пароля название учетной записи, фамилию или имя пользователя, а также легко угадываемые сочетания символов.

8.7 Пользователь несет персональную ответственность за сохранение в тайне основного пароля. Запрещается сообщать пароль другим лицам, записывать его, а также пересылать открытым текстом в электронных сообщениях.

8.8 Пользователь обязан не реже одного раза в четыре месяца производить смену основного пароля соблюдая требования настоящего положения.

8.9 В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом в **ИАГ ОПР** и изменить основной пароль.

8.10 Восстановление скомпрометированного или забытого основного пароля пользователя осуществляется системным администратором путем изменения (сброса) основного пароля пользователя на первичный пароль на основании письменной заявки пользователя (**Приложение №2**).

8.11 Устная заявка пользователя на изменение пароля не является основанием для проведения таких изменений.

8.12 Для предотвращения угадывания паролей системный администратор обязан настроить механизм блокировки учетной записи при трехкратном неправильном вводе пароля.

8.13 Разблокирование учетной записи пользователя осуществляется системным администратором на основании заявки владельца учетной записи (**Приложение №2**).

9. ДОСТУП К РЕСУРСАМ ИНТЕРНЕТ

9.1 Всем сотрудникам Учреждения для исполнения задач, связанных с производственной деятельностью предоставляется доступ к ресурсам Интернет. Доступ к ресурсам Интернет в других целях – **ЗАПРЕЩЕН**.

9.2 Доступ к ресурсам Интернет, связанный со служебной необходимостью, предоставляется без ограничений.

9.3 Системный администратор обязан не реже одного раза в месяц предоставлять отчет об использовании Интернет ресурсов сотрудниками Учреждения директору Учреждения.

9.4 Доступ к ресурсам Интернет может быть блокирован системным администратором без предварительного уведомления, при возникновении нештатных ситуаций, либо в иных случаях, предусмотренных организационными документами, приказами, постановлениями, положениями и иными распоряжениями руководства Учреждения.

9.5 Правила работы в сети интернет описаны в (**Приложении №3**)

10. ЭЛЕКТРОННАЯ ПОЧТА

10.1 Для исполнения задач, связанных со служебной деятельностью сотрудникам Учреждения может быть предоставлен доступ к системе электронной почты. Использование системы электронной почты в других целях – **ЗАПРЕЩЕНО**.

10.2 Доступ к системе электронной почты предоставляется сотруднику Учреждения на основании утвержденной **ЗАЯВКИ** (**Приложение №1**) на имя директора Учреждения.

10.3 Электронная почта является собственностью Учреждения и может быть использована **ТОЛЬКО** в служебных целях. Использование электронной почты в других целях категорически **ЗАПРЕЩЕНО**.

10.4 Использование электронной почты других компаний в служебных целях, **ЗАПРЕЩЕНО**.

10.5 Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя Учреждения.

10.6 В случае обнаружения значительных отклонений в параметрах работы средств обеспечения работы системы электронной почты, системный администратор обязан немедленно сообщить об этом руководителю **ИАГ ОПР** для принятия решений.

10.7 Доступ к серверу электронной почты может быть блокирован системным администратором без предварительного уведомления, при

возникновении нештатных ситуаций, либо в иных случаях, предусмотренных организационными документами.

10.8 Правила работы с электронной почтой описаны в (**Приложении №4**)

11. АНТИВИРУСНАЯ ЗАЩИТА

11.1 К использованию допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

11.2 Установка средств антивирусного контроля на компьютерах (серверах ЛВС) Учреждения осуществляется системными администраторами.

11.3 Настройка параметров средств антивирусного контроля осуществляется системным администраторов в соответствии с руководствами по применению конкретных антивирусных средств. Изменение настроек другими сотрудниками **ЗАПРЕЩЕНО**.

11.4 Антивирусное средство ежедневно в начале работы при загрузке компьютера (для серверов ЛВС – при перезапуске) в автоматическом режиме проводит антивирусный контроль всех дисков и файлов систем.

11.5 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах, CD–ROM и т.п.).

11.6 **Антивирусная проверка должна проводиться:**

- на компьютерах сотрудников – не реже одного раза в неделю;
- на серверах ЛВС – не реже двух раз в неделю.

11.7 При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно или вместе с

системным администратором должен провести внеочередной антивирусный контроль своей рабочей станции.

12. ХРАНЕНИЕ ДАННЫХ

12.1 Сотрудники **ОБЯЗАНЫ** хранить служебную информацию только для общего пользования (документы, электронные таблицы, презентации и т.д.) на корпоративном портале совместной работы (ONLY OFFICE).

12.2 При трудоустройстве каждому сотруднику для хранения служебной информации выделяется именная сетевая папка на сервере объемом 2 гигабайта.

12.3 В случае необходимости объем предоставленного места в сетевой папке на сервере может быть увеличен на основании утвержденной **ЗАЯВКИ** (**Приложение №1**), либо может быть предоставлен внешний накопитель для хранения данных на основании **СЛУЖЕБНОЙ ЗАПИСКИ**.

12.4 Хранение служебной информации на компьютерах сотрудников **ЗАПРЕЩЕНО**, исключением является служебная информация для временного использования, не более 90 дней с последующим удалением или переносом на корпоративный портал, а также информация необходимая для функционирования такой системы как ЕИАС ФСТ и подобной ей, АРМ Банк–клиент и подобной ей, Контур–Экстерн и подобной ей, почтовом клиенте.

12.5 Хранение любой личной информации сотрудников Учреждения в сетевых папках **ЗАПРЕЩЕНО**.

12.6 Организация сетевых папок на рабочих станциях сотрудников Учреждения **ЗАПРЕЩЕНО**.

12.7 Для обеспечения целостности данных находящихся на серверном оборудовании системным администраторам необходимо проводить резервное копирование не реже одного раза в сутки.

12.8 Резервное копирование **ИНФОРМАЦИИ НАХОДЯЩЕЙСЯ НА ПЕРСОНАЛЬНОМ КОМПЬЮТЕРЕ СОТРУДНИКА УЧРЕЖДЕНИЯ**

ИЛИ ПРЕДОСТАВЛЕННОМ ВНЕШНЕМ НАКОПИТЕЛЕ НЕ ПРЕДУСМОТРЕНО.

12.9 Восстановление утерянной информации, находящейся на персональном компьютере сотрудника или на вышедшем из строя внешнем накопителе **НЕВОЗМОЖНО**.

13. УСТАНОВКА И ОБСЛУЖИВАНИЕ ОБОРУДОВАНИЯ

13.1 Установка и обслуживание оборудования возможна только системным администратором.

13.2 Установка и обслуживание оборудования сотрудниками других отделов **ЗАПРЕЩЕНА**.

14. УСТАНОВКА И ОБСЛУЖИВАНИЕ ПРОГРАММ

14.1 Установка разрешенных для использования программ возможна только системным администратором.

14.2 Установка программ сотрудниками других отделов **ЗАПРЕЩЕНА**.

14.3 Решение о включении(/исключении) программы в(/из) список(а) разрешенного программного обеспечения принимает начальник **ОПР** и руководитель **ИАГ ОПР**, утверждает директор Учреждения.

14.4 Программное обеспечение, разрешенное для использования на рабочих станциях и серверах, утверждается Директором Учреждения в (**Приложение №5**).

Приложение №1

НОУ ДПО УМЦ
НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
УЧЕБНО-МЕТОДИЧЕСКИЙ ЦЕНТР

Фактический адрес: 650000, Российская Федерация, г. Кемерово, ул. Шестакова, 6
Почтовый адрес: 650000, Российская Федерация, г. Кемерово, пр. Кузнецкий, 17, оф. 206
Телефон/факс: 8(3842) 45-41-11, 36-56-05, 36-58-12, E-mail: umc.pk@mail.ru Web: www.umc-kem.ru
ОКПО 85223316, ОГРН 1084200002260, ИНН/КПП 4205152080/420501001

Директору
НОУ ДПО «УМЦ»
Е.П. Лодза

_____
(ФИО)
_____
(должность)
_____
_____
(структурное подразделение)

№_____ от «___» _____ 20___ г.

ЗАЯВКА

на внесение изменений в списки пользователей автоматизированной системы и наделения пользователей полномочиями доступа к ресурсам

Прошу [ ] зарегистрировать / [ ] исключить / [ ] предоставить полномочия / [ ] лишить полномочий **пользователя автоматизированной системы** (нужное выделить [V])

_____
_____
_____
_____
(фамилия имя отчество, должность с указанием подразделения)

для решения задач:

[ ] работа на / [ ] администрирование **рабочей станции;**

[ ] работа / [ ] администрирование проектов / [ ] администрирование документов **на корпоративном портале;**

[ ] работа с / [ ] администрирование **электронной почты(ой);**

[ ] работа с / [ ] администрирование **сайта(ом);**

[ ] увеличение объема **сетевой папки до ____ гигабайт;**

[ ] администрирование **сетевого оборудования;**

[ ] работа / [ ] администрирование **серверного оборудования;**

[ ] администрирование **системы антивирусной защиты;**

[ ] администрирование **системы видеонаблюдения.**

_____ / _____ « » 20 г.
подпись ФИО дата

Согласовано:

Начальник отдела перспективного развития:

_____ / _____ « » 20 г.
подпись ФИО дата

Начальник отдела по работе с персоналом:

_____ / _____ « » 20 г.
подпись ФИО дата

Руководитель структурного подразделения по направлению деятельности:

_____ / _____ « » 20 г.
подпись ФИО дата

Приложение №2

НОУ ДПО УМЦ
НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
УЧЕБНО-МЕТОДИЧЕСКИЙ ЦЕНТР

Фактический адрес: 650000, Российская Федерация, г. Кемерово, ул. Шестакова, 6
Почтовый адрес: 650000, Российская Федерация, г. Кемерово, пр. Кузнецкий, 17, оф. 206
Телефон/факс: 8(3842) 45-41-11, 36-56-05, 36-58-12, E-mail: umc.pk@mail.ru Web: www.umc-kem.ru
ОКПО 85223316, ОГРН 1084200002260, ИНН/КПП 4205152080/420501001

Директору
НОУ ДПО «УМЦ»
Е.П. Лодза

_____
(ФИО)

_____
(должность)

_____

№_____ от «___» _____ 20___ г.

_____
(структурное подразделение)

ЗАЯВКА

на сброс пароля или разблокировку учетной записи

Прошу [ ] сбросить пароль / [ ] разблокировать учетную запись **пользователя автоматизированной системы,** [ ] сбросить пароль от ящика электронной почты, [ ] сбросить пароль пользователя корпоративного портала (нужное выделить [V])

_____

_____

_____

(фамилия имя отчество, должность с указанием подразделения)

_____/_____ « » 20 г.

подпись ФИО дата

Согласовано:

Руководитель структурного подразделения:

_____/_____ « » 20 г.

подпись	ФИО	дата

Начальник отдела перспективного развития:

подпись	ФИО	дата

Исполнено:

Ответственный сотрудник информационно – аналитической группы отдела перспективного развития:

/	« »	20 г.
подпись	ФИО	дата

Приложение №3

НОУ ДПО УМЦ
НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
УЧЕБНО-МЕТОДИЧЕСКИЙ ЦЕНТР

Фактический адрес: 650000, Российская Федерация, г. Кемерово, ул. Шестакова, 6
Почтовый адрес: 650000, Российская Федерация, г. Кемерово, пр. Кузнецкий, 17, оф. 206
Телефон/факс: 8(3842) 45-41-11, 36-56-05, 36-58-12, E-mail: umc.pk@mail.ru Web: www.umc-kem.ru
ОКПО 85223316, ОГРН 1084200002260, ИНН/КПП 4205152080/420501001

ПРАВИЛА РАБОТЫ
С РЕСУРСАМИ СЕТИ ИНТЕРНЕТ

Глобальная сеть Интернет предоставляет доступ к ресурсам различного содержания и направленности. Информационно – аналитическая группа отдела перспективного развития оставляет за собой право ограничивать доступ к ресурсам сети Интернет, содержание которых не имеет отношения к исполнению служебных обязанностей, а так же к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.

При работе с ресурсами сети Интернет недопустимо:

• разглашение коммерческой и служебной информации, ставшей известной сотруднику компании по служебной необходимости либо иным путем;

• распространение защищаемых авторскими правами материалов, затрагивающих какой–либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;

• публикация, загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также размещения ссылок на вышеуказанную информацию;

При работе с ресурсами Интернет запрещается:

• загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом.

• использовать программные и аппаратные средства, позволяющие получить доступ к ресурсу, запрещенному к использованию политикой компании.

Возможность получить доступ к ресурсу не является гарантией того, что запрошенный ресурс является разрешенным корпоративной политикой Учреждения. Вся информация о ресурсах, посещаемых сотрудниками Учреждения, протоколируется и, при необходимости, может быть предоставлена руководителям подразделений, а также директору Учреждения для детального изучения.

Приложение №4

НОУ ДПО УМЦ
НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
УЧЕБНО-МЕТОДИЧЕСКИЙ ЦЕНТР

Фактический адрес: 650000, Российская Федерация, г. Кемерово, ул. Шестакова, 6
Почтовый адрес: 650000, Российская Федерация, г. Кемерово, пр. Кузнецкий, 17, оф. 206
Телефон/факс: 8(3842) 45-41-11, 36-56-05, 36-58-12, E-mail: umc.pk@mail.ru Web: www.umc-kem.ru
ОКПО 85223316, ОГРН 1084200002260, ИНН/КПП 4205152080/420501001

ПРАВИЛА РАБОТЫ С ЭЛЕКТРОННОЙ ПОЧТОЙ

Электронная почта является собственностью Учреждения и может быть использована **ТОЛЬКО** в служебных целях. Использование электронной почты в других целях категорически запрещено.

Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя.

При работе с корпоративной системой электронной почты сотрудникам Учреждения запрещается:

- использовать адрес корпоративной почты для оформления подписок и массовых рассылок;
- публиковать свой адрес, либо адреса других сотрудников Учреждения на общедоступных Интернет ресурсах (форумы, конференции и т.п.);
- отправлять сообщения с вложенными файлами общий объем которых превышает 30 Мегабайт.
- открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами, даже если отправитель письма хорошо известен;
- осуществлять массовую рассылку почтовых сообщений (более 10) сотрудникам сторонних организаций без их на то согласия. Данные действия квалифицируются как **СПАМ** и являются незаконными.

• осуществлять массовую рассылку почтовых сообщений рекламного характера.

• рассылка через электронную почту материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также ссылки на вышеуказанную информацию;

• распространение защищаемых авторскими правами материалов, затрагивающих какой–либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны.

• распространять информацию содержание и направленность которой запрещены международным и Российским законодательством включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.

• распространять информацию ограниченного доступа, представляющую коммерческую тайну;

•предоставлять, кому быто ни было пароль доступа к своему почтовому ящику.

Приложение №5

НОУ ДПО УМЦ
НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
УЧЕБНО-МЕТОДИЧЕСКИЙ ЦЕНТР

Фактический адрес: 650000, Российская Федерация, г. Кемерово, ул. Шестакова, 6
Почтовый адрес: 650000, Российская Федерация, г. Кемерово, пр. Кузнецкий, 17, оф. 206
Телефон/факс: 8(3842) 45-41-11, 36-56-05, 36-58-12, E-mail: umc.pk@mail.ru Web: www.umc-kem.ru
ОКПО 85223316, ОГРН 1084200002260, ИНН/КПП 4205152080/420501001

Директору

НОУ ДПО «УМЦ»

Е.П. Лодза

_____
(ФИО)

_____
(должность)

_____

_____
(структурное подразделение)

№_____ от «___» _____ 20___ г.

Список разрешенного программное обеспечения для установки и использования на рабочих станциях и серверах на 01 Января 2017г.

№ п/п	Наименование программного обеспечения

_____/ « » 20 г.
подпись ФИО дата

Согласовано:

Начальник отдела перспективного развития:

_____/ « » 20 г.
подпись ФИО дата

Руководитель информационно – аналитической группы отдела перспективного развития:

_____ /		« »	20 г.
подпись	ФИО		дата

Приложение №6

НОУ ДПО УМЦ
НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
УЧЕБНО-МЕТОДИЧЕСКИЙ ЦЕНТР

Фактический адрес: 650000, Российская Федерация, г. Кемерово, ул. Шестакова, 6
Почтовый адрес: 650000, Российская Федерация, г. Кемерово, пр. Кузнецкий, 17, оф. 206
Телефон/факс: 8(3842) 45-41-11, 36-56-05, 36-58-12, E-mail: umc.pk@mail.ru Web: www.umc-kem.ru
ОКПО 85223316, ОГРН 1084200002260, ИНН/КПП 4205152080/420501001

Директору

НОУ ДПО «УМЦ»

_____Е.П. Лодза

«___» _____ 20___г.

_____
(ФИО)

_____
(должность)

_____

_____
(структурное подразделение)

№_____ от «___» _____ 20___ г.

ЖУРНАЛ

регистрации заявок, поступающих в информационно аналитическую группу отдела перспективного развития за _____ месяц 2017 года.

№ п/п	Номер заявки	Тип заявки	Дата – время

/ « » 20 г.

подпись ФИО дата

Согласовано:

Начальник отдела перспективного развития:

подпись ФИО дата