Федеральное государственное бюджетное образовательное учреждение
высшего образования
«АСТРАХАНСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ»
Министерства здравоохранения Российской Федерации
(ФГБОУ ВО Астраханский ГМУ Минздрава России)

ПРИКАЗ

«29» сентября 2020 г. № 298

Астрахань

Об утверждении Порядка администрирования и предоставления прав доступа пользователей к информационным системам, сервисам и ресурсам ФГБОУ ВО Астраханский ГМУ Минздрава России

В соответствии с положениями Федеральных законов от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», в целях обеспечения безопасности информационных систем, сервисов и ресурсов ФГБОУ ВО Астраханский ГМУ Минздрава России,

Приказываю:

1. Утвердить и ввести в действие с момента подписания приказа Порядок администрирования и предоставления прав доступа пользователей к информационным системам, сервисам и ресурсам ФГБОУ ВО Астраханский ГМУ Минздрава России (Приложение № 1).

2. Проректорам и руководителям структурных подразделений Университета:

2.1. Довести настоящий приказ до сведения подчиненных сотрудников. Копии листов ознакомления направить в отдел информационной безопасности в срок до 01.11.2020 (Приложение № 2).

2.2. При необходимости предоставления (изменения) доступа подчиненных сотрудников к информационным системам, сервисам и ресурсам Университета, руководствоваться настоящим приказом.

3. Начальнику управления по печати, медиа и информационным технологиям (Иванчук О.В.) разместить настоящий приказ на официальном сайте Университета в разделе «Документы/Локальные нормативные акты». Приложения №№ 1, 2, 3 к Порядку дополнительно разместить на официальном

сайте Университета в разделах «Сотрудникам/Техническая поддержка», «О ВУЗе/Документы/Прочие документы/Шаблоны документов».

4. Начальнику отдела делопроизводства (Елизаровой Л.Ю.) ознакомить с настоящим приказом всех заинтересованных лиц.

5. Настоящий приказ вступает в силу с момента подписания.

6. Контроль за исполнением настоящего приказа возложить на проректора по общественной и информационной безопасности С.А. Авдеева.

Ректор
д.м.н., профессор О.А. Башкина

Приложение № 1
к приказу
№ 298
от «29» 09 2020 года

Утверждаю
Ректор ФГБОУ ВО
Астраханский ГМУ
Минздрава России

_____ О.А. Башкина
«___» _____2020 г.

ПОРЯДОК
администрирования и предоставления прав доступа пользователей к информационным системам, сервисам и ресурсам ФГБОУ ВО Астраханский ГМУ Минздрава России

Астрахань 2020

1. Общие положения

1.1. В целях обеспечения безопасности информационных систем, сервисов и ресурсов ФГБОУ ВО Астраханский ГМУ Минздрава России (далее – Университет), соблюдения принципа персональной ответственности пользователей за свои действия, авторизованный доступ пользователей к информационным системам, сервисам и ресурсам Университета обеспечивается на основе зарегистрированных персональных учетных записей, которые являются уникальными идентификаторами пользователей.

1.2. Под «пользователем» понимается одно физическое лицо, которому необходим доступ к определенным информационным системам, сервисам и ресурсам Университета.

1.3. Организационное и техническое обеспечение процессов изменения полномочий (предоставление/изменение/прекращение прав доступа) возлагается:

1.3.1. В информационных системах платформы «1С» («1С:Университет», «1С:Бухгалтерия», «1С:Зарплата и кадры»), на электронном почтовом сервере Университета – на отдел информационной безопасности.

1.3.2. В сервисах и разделах ограниченного доступа, размещенных на официальном сайте Университета в информационно-телекоммуникационной сети «Интернет» (astgmu.ru), на образовательном портале Университета (portal.astgmu.ru) – на отдел IT-менеджмента и цифрового обеспечения.

1.3.3. Доступ к информационно-телекоммуникационной сети «Интернет» через прокси-сервер Университета, справочным ресурсам и файлообменнику – на отдел технической поддержки.

1.4. Положения настоящего Порядка администрирования и предоставления прав доступа пользователей к информационным системам, сервисам и ресурсам ФГБОУ ВО Астраханский ГМУ Минздрава России (далее – Порядок) должны анализироваться отделом информационной безопасности не реже одного раза в год. В случае если в ходе такого анализа была установлена необходимость внесения изменений в Порядок, новая редакция Порядка разрабатывается руководителем отдела информационной безопасности, либо, по его указанию, соответствующим специалистом того же отдела.

2. Область применения

2.1 Настоящий Порядок регламентирует действия по:

- предоставлению доступа к информационным системам, сервисам и ресурсам Университета;
- созданию, блокировке/аннулированию учетных записей пользователей, а также внесению изменений в разрешения учетных записей пользователей информационных систем, сервисов и ресурсов Университета.

2.2 Требования настоящего Порядка обязательны для выполнения во всех структурных подразделениях Университета.

3. Требования к учетным записям пользователей и парольной защите

3.1. Не допускается создание не персонифицированных, групповых и анонимных учетных записей пользователей. Использование несколькими сотрудниками Университета одного и того же имени пользователя запрещено, за исключением отдельных учетных записей пользователей электронного почтового сервера Университета по согласованию с отделом информационной безопасности.

3.2. Пользователи информационных систем, сервисов и ресурсов Университета должны осуществлять подключение к ним только с использованием собственных учетных данных для авторизации (логин и пароль). Подключение с использованием чужих учетных записей (логинов и паролей) не допускается.

3.3. При создании новой учетной записи первоначальное значение пароля устанавливается администратором соответствующей информационной системы, сервиса или ресурса, указанным в п. 1.3 настоящего Порядка.

3.4. Соответствующая информационная система, сервис или ресурс настраиваются таким образом, чтобы после первоначального входа пользователю была предоставлена возможность установления собственного личного пароля. При отсутствии такой возможности создание/изменение личного пароля осуществляется администратором соответствующей информационной системы, сервиса или ресурса, в том числе в случае соблюдения периодичности смены личных паролей, принятых в Университете.

3.5. Периодичность смены паролей пользователей информационных систем, сервисов и ресурсов должна составлять не реже одного раза в 90 дней. Исключение могут составлять информационные ресурсы, где такая возможность со стороны пользователя не предусмотрена.

3.6. В целях обеспечения криптоустойчивости паролей, предотвращения возможности их угадывания либо подбора, в том числе с помощью специализированного программного обеспечения, личные пароли пользователей информационных систем, сервисов и ресурсов Университета должны удовлетворять следующим требованиям:

3.6.1. Длина пароля должна быть не менее 8 символов.

3.6.2. В числе символов пароля должны присутствовать три из четырех видов символов:

- буквы в верхнем регистре;
- буквы в нижнем регистре;
- цифры;
- специальные символы (! @ # $ % ^ & * ( ) - _ + = ~ [ ] { } | \ : ; ' " < > , . ? /).

3.6.3. Пароль не должен содержать легко вычисляемые сочетания символов, например:

- собственные имена, фамилии, номера телефонов, даты;
- последовательно расположенные на клавиатуре символы («1234», «QWERTY», и т.п.);
- общепринятые сокращения («USER», «TEST» и т.п.);
- повседневно используемое или распространенное слово (имена или фамилии друзей, коллег, актеров или сказочных персонажей, клички животных);
- что-либо из вышеперечисленного в обратном написании или с добавлением цифр в начале или конце слова.

3.6.4. При смене пароля значение нового пароля должно отличаться от предыдущего не менее чем в 4 позициях.

3.6.5. Для различных информационных систем, сервисов и ресурсов необходимо устанавливать собственные, отличающиеся пароли.

3.7. Рекомендации и примеры по созданию собственного крипоустойчивого пароля приведены в приложении № 1 к Порядку.

3.8. В случае, если данные для авторизации пользователя становятся общедоступными (являются скомпрометированными), либо имеется основание подозревать о возможной компрометации учетных данных, пользователь обязан незамедлительно сообщить о данном факте непосредственному руководителю и в отдел информационной безопасности.

3.9. Пользователь несет персональную ответственность в соответствии с законодательством и внутренними нормативными актами Университета за свои действия, послужившие причиной компрометации данных для авторизации в информационных системах, сервисах и ресурсах Университета.

4. Предоставление (изменение) доступа к информационным системам, сервисам и ресурсам

4.1. Для предоставления доступа пользователю к информационным системам, сервисам и ресурсам Университета необходимо выполнение одного из следующих условий:

- доступ необходим для выполнения пользователем должностных обязанностей в соответствии со своей должностной инструкцией (для работников Университета);
- доступ необходим для выполнения пользователем обязанностей другого пользователя по указанию (в виде приказа или распоряжения) руководства Университета (для работников Университета);
- доступ необходим для обеспечения информированности пользователя о ходе и результатах образовательного процесса, доступа к библиотечному фонду, участия в проведении тестовых, контрольных работ или иного итогового/промежуточного контроля образовательного процесса (для обучающихся Университета);

- доступ необходим для выполнения пользователем работ в ходе реализации контрактов (договоров), заключенных Университетом (для работников сторонних организаций).

4.2. Основанием для предоставления/изменения прав доступа к информационным системам, сервисам и ресурсам Университета является подписанная соответствующими ответственными лицами Заявка, оформленная по установленной форме (приложения №№ 2, 3 к Порядку). Актуальные формы Заявок размещаются на официальном сайте Университета (astgmu.ru) в разделах «Сотрудникам/Техническая поддержка», «О ВУЗе/Документы/Прочие документы/Шаблоны документов».

4.3. Ответственность за содержание, полноту, достоверность и своевременное представление информации, указанной в Заявке, возлагается на ответственное лицо, подписавшее Заявку.

4.4. Рассмотрение Заявки осуществляется администратором соответствующей информационной системы, сервиса или ресурса, указанным в п. 1.3 настоящего Порядка, в течении двух рабочих дней. Учетные данные для доступа к информационным системам, сервисам и ресурсам (логин и пароль) выдаются пользователю лично, под роспись. Пользователь в обязательном порядке ознакамливается с требованиями по информационной безопасности (приложение № 4 к Порядку). Сведения о выдаче учетной записи пользователя и ознакомлении с требованиями информационной безопасности заносятся в Журнал учета идентификационных данных пользователей информационных систем, сервисов и ресурсов (приложение № 5 к Порядку).

4.5. В случае если доступ к информационной системе, сервису или ресурсу согласно Заявке по какой-либо причине не может быть предоставлен, Заявка возвращается инициатору с подробным описанием данной причины.

5. Аннулирование/блокирование доступа к информационным системам, сервисам и ресурсам

5.1. Аннулирование/блокирование доступа пользователя к ресурсам происходит в случаях:

- изменения должностных обязанностей пользователя;
- длительного обоснованного периода отсутствия (например, декретный отпуск, отпуск по уходу за ребенком);
- нарушения пользователем правил доступа к ресурсу;
- увольнение пользователя;
- по иным распоряжениям ректора Университета.

Аннулирование/блокирование доступа должно быть инициировано не позднее пяти рабочих дней с момента возникновения соответствующего события.

5.2. Обязанности по инициированию аннулирования/блокирования доступа пользователя к ресурсам возлагаются на руководителя соответствующего структурного подразделения Университета.

5.3. Информация об инициировании аннулирования/блокирования доступа (с указанием причины) направляется администратору соответствующей информационной системы, сервиса или ресурса в произвольной форме в письменном виде за подписью руководителя соответствующего структурного подразделения Университета.

5.4. Аннулирование/блокирование доступа осуществляется администратором соответствующей информационной системы, сервиса или ресурса, указанным в п. 1.3. настоящего Положения.

5.5. Сведения об аннулировании/блокировании учетной записи пользователя заносятся в Журнал учета идентификационных данных пользователей информационных систем, сервисов и ресурсов.

Приложение № 2
к приказу
№ _____
от «___» _____ 2020 года

ЛИСТ ОЗНАКОМЛЕНИЯ

работников _____
(наименование структурного подразделения Университета)
_____

с приказом от «___» _____ 2020 года № _____ и Порядком администрирования и предоставления прав доступа пользователей к информационным системам, сервисам и ресурсам ФГБОУ ВО Астраханский ГМУ Минздрава России.

№ п/п	ФИО, должность	Дата	Подпись

Приложение № 1
к Порядку администрирования и предоставления прав доступа пользователей к информационным системам, сервисам и ресурсам ФГБОУ ВО Астраханский ГМУ Минздрава России

Рекомендации пользователю по выбору личного пароля

Личный пароль к информационным системам, сервисам и ресурсам Университета, отвечающий требованиям криптойстойчивости, можно создать следующими способами:

1) Сформировать пароль с помощью генератора паролей посредством соответствующих он-лайн сервисов (например на ресурсе https://passgenerator.ru);

Он-лайн сервисы при создании паролей позволяют установить требования к нему по длине и используемым символам.

Плюсом такого способа является достаточная надежность и криптоустойчивость пароля.

Недостатком является трудность их запоминания, в том числе, с учетом необходимости использования различных паролей для разных информационных систем. Практика показывает, что в данном случае пользователи в большинстве своем записывают такие пароли на материальные носители, что повышает риски их компрометации.

2) Сформировать пароль самостоятельно по следующему алкгоритму:

- придумать нелогичную смешную фразу, которую легко запомнить. Например, «Усталый студент гладит дорогу»;
- выбрать первые три буквы из каждого слова фразы – «устстугладор»;
- набрать полученную последовательность в английской раскладке клавиатуры – «ecncneukfljh», это основа будущего пароля;
- выбрать номер (или номера) буквы, которая будет записываться в верхнем регистре и после которой будет стоять специальный символ или цифра. Например, это будет четвертая буква, а в качестве специального символа выбран «#». Получаем: «ecnC#neukfljh».

Плюсом такого способа является достаточная надежность и криптоустойчивость пароля. Также данный способ позволяет сформировать запоминаемые пароли для разных информационных систем. Даже в случае, если пароль забыт, используемый алгоритм позволяет достаточно легко его вспомнить.

Недостатков у данного способа практически не имеется.

Примечание.

Пароли длиной от 1 до 6 символов обычный персональный компьютер способен обработать за несколько минут. Удлинение пароля до 8 символов увеличит срок обработки до несколько дней. Еще несколько дополнительных символов в пароле заставят метод обычного подбора работать годами. Самыми практичными и надежными считаются пароли длиной 11-12 символов в разных регистрах, с использованием цифр и прочих символов.

Приложение № 2
к Порядку администрирования и предоставления прав доступа пользователей к информационным системам, сервисам и ресурсам ФГБОУ ВО Астраханский ГМУ Минздрава России

Кому:
Начальнику отдела
информационной безопасности

_____
Ф.И.О.

ЗАЯВКА

на предоставление доступа к информационным ресурсам платформы 1С, электронному почтовому сервер ФГБОУ ВО Астраханский ГМУ Минздрава России

Прошу предоставить сотруднику:

ФИО сотрудника	
Контактный телефон	

доступ к следующим информационным ресурсам Университета:

№	Наименование сервиса (ресурса)*		Права доступа
1.	1С: Университет		
2.	1С: Бухгалтерия		
3.	1С: Зарплата и кадры		
4.	Электронный почтовый сервер		
5.	Иное (вписать)		

** отметить знаком «Х» необходимые сервисы, права доступа – указать в зависимости от необходимости выполнения работы согласно должностной инструкции (полный доступ, общий доступ или какое-либо конкретное направление).*

Обоснование предоставления доступа** _____
_____
_____

*** - указывается основание для предоставления соответствующих прав доступа (например - согласно должностным инструкциям).*

ФИО Руководителя	
Должность	
Контактный телефон	

Дата _____ Подпись _____/_____/

Бланк для передачи в отдел технической поддержки

В соответствии с заявкой и предоставленным доступом прошу обеспечить техническую возможность подключения АРМ пользователя _____
к ИС _____.

Начальник отдела
информационной безопасности _____ /_____/

Бланк для выдачи сотруднику

Учетная запись сотрудника (логин)	
Пароль	

Учетные данные (логин/пароль) сотрудник получает в отделе информационной безопасности лично под роспись.

Приложение № 3
к Порядку администрирования и предоставления прав доступа пользователей к информационным системам, сервисам и ресурсам ФГБОУ ВО Астраханский ГМУ Минздрава России

Кому:
Начальнику управления по печати, меди и информационным технологиям

_____
Ф.И.О.

СОГЛАСОВАНО
Начальник отдела
информационной безопасности
_____/_____/
подпись, Ф.И.О.

ЗАЯВКА
на предоставление доступа к информационным сервисам и ресурсам ФГБОУ ВО Астраханский ГМУ Минздрава России

Прошу предоставить сотруднику:

ФИО сотрудника	
Контактный телефон	

доступ к следующим информационным сервисам и ресурсам Университета:

№	Наименование сервиса (ресурса)*	
1.	сеть Интернет	
2.	Образовательный портал АГМУ	
3.	Электронный дневник	
4.	Консультант-Плюс	
5.	Файловый обменник	
6.	Иное (вписать)	

* *отметить знаком «Х» необходимые сервисы*

ФИО Руководителя	
Должность	
Контактный телефон	

Дата _____ Подпись _____/_____/

--------✂--------✂----------✂----------✂----------✂----------✂----------✂--------✂--------✂--------

Бланк для выдачи сотруднику

Сеть Интернет:

Сетевое имя сотрудника (логин**)	
Пароль	

** - учетная запись для терминального входа, и/или на прокси-сервер для доступа в Интернет.

Другие сервисы и ресурсы:

Учетная запись сотрудника (логин)	
Пароль	

Учетные данные (логин/пароль) сотрудник получает в управлении по печати, меди и цифровым технологиям лично под роспись.

Приложение № 4
к Порядку администрирования и предоставления прав доступа пользователей к информационным системам, сервисам и ресурсам ФГБОУ ВО Астраханский ГМУ Минздрава России

Лист ознакомления с основными требованиями информационной безопасности при работе с информационными системами, сервисами и ресурсами Университета

Я, _____
_____, ознакомлен с основными требованиями информационной безопасности при работе с информационными системами, сервисами и ресурсами Университета, а именно уведомлен о том, что пользователь

ОБЯЗАН:

- использовать и своевременно менять пароли доступа к информационным системам, сервисам и ресурсам в соответствии с периодичностью, установленной внутренними нормативными актами Университета;
- в случае подозрения на то, что пароль стал кому-либо известен (скомпрометирован), поменять пароль и сообщить о факте компрометации непосредственному руководителю и в отдел информационной безопасности;
- незамедлительно сообщить в отдел информационной безопасности в случае получения от кого-либо просьбы сообщить пароль доступа к информационным ресурсам Университета;
- при применении внешних носителей информации (например флеш-карт) перед началом работы провести их проверку на предмет наличия компьютерных вирусов средствами антивирусной защиты персонального компьютера.

Пользователю ЗАПРЕЩАЕТСЯ:

- передавать или иным способом сообщать другим лицам, в том числе другим сотрудникам Университета, личные идентификационные данные (логин/пароль);
- хранить записанные или иным способом размещенные на материальном носителе личные идентификационные данные (логин/пароль) в легкодоступном месте;
- указывать пароль доступа к информационным ресурсам Университета в сообщениях электронной почты;
- использовать один и тот же пароль для доступа к различным информационным ресурсам;
- использовать персональный компьютер, периферийное оборудование (принтеры, сканеры и т.п.), а также компоненты программного и аппаратного обеспечения не по назначению (в неслужебных целях);
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств персонального компьютера или устанавливать дополнительно любые программные и аппаратные средства;
- осуществлять обработку конфиденциальной информации, в том числе персональных данных, в присутствии посторонних (не допущенных к данной информации) лиц;
- оставлять включенным без присмотра свой персональный компьютер, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры – комбинации клавиш Win + «L» или Ctrl + Alt + Delete);
- оставлять без личного присмотра на рабочем месте или где бы то ни было носители конфиденциальной информации, в том числе содержащие персональные данные;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушениям информационной безопасности персональных данных.

Дата _____ Подпись _____/_____/

Приложение № 5
к Порядку администрирования и предоставления прав доступа пользователей к информационным системам, сервисам и ресурсам ФГБОУ ВО Астраханский ГМУ Минздрава России

ЖУРНАЛ
учета идентификационных данных пользователей информационных систем, сервисов и ресурсов ФГБОУ ВО Астраханский ГМУ Минздрава России

№ п/п	ФИО сотрудника, должность	Наименование ИС (ИР)	Права доступа	Логин	Роспись в получении ИД, дата	Отметка об аннулировании/ блокировании ИД	Примечание