МИНИСТЕРСТВО ПО ИНФОРМАТИЗАЦИИ, СВЯЗИ И ВОПРОСАМ ОТКРЫТОГО УПРАВЛЕНИЯ ТУЛЬСКОЙ ОБЛАСТИ

П Р И К А З

19.08.2019 **№ 88-осн**

Об утверждении Регламента по организации парольной защиты в региональных информационных системах Тульской области

В соответствии с приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», нормативно-методическим документом «Меры защиты информации в государственных информационных системах», утвержденным приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2014 года,

п р и к а з ы в а ю :

1. Утвердить Регламент по организации парольной защиты в региональных информационных системах Тульской области (Приложение).
2. Признать утратившими силу:

приказ министерства по информатизации, связи и вопросам открытого управления Тульской области от 20.02.2015 № 12-осн «Об утверждении Инструкции по авторизации пользователей в информационных системах органов исполнительной власти и аппарата правительства Тульской области»;

приказ министерства по информатизации, связи и вопросам открытого управления Тульской области от 25.04.2016 № 54-осн «Об утверждении Инструкции по авторизации пользователей подведомственных учреждений Тульской области в информационных системах органов исполнительной власти и аппарата правительства Тульской области».

3. Контроль за исполнением приказа оставляю за собой.
4. Приказ вступает в силу со дня подписания.

Министр по информатизации, связи и вопросам открытого управления Тульской области

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат:051991C1290C008982E811C5CA9EC51B5C
Владелец:Раков Ярослав Юрьевич
Действителен с 08.10.2018 по 08.10.2019

Я.Ю. Раков

исп.: Баранов Михаил Николаевич, Кочетова Дарья Александровна
тел. 24-52-16

Приложение
к приказу министерства по информатизации,
связи и вопросам открытого управления
Тульской области
от «___» _____ 20____ г. № _____

РЕГЛАМЕНТ
по организации парольной защиты в региональных информационных системах Тульской области

I. Общие положения

1. Настоящий Регламент определяет порядок доступа пользователей к ресурсам региональной информационной системы Тульской области (далее – РИС ТО), принципы идентификации и аутентификации, правила разработки таблиц допуска к информационным ресурсам РИС ТО и контроль за действиями пользователей при работе с паролями.

2. Действие настоящего Регламента распространяется на организации – участники информационного взаимодействия РИС ТО (далее – УИВ РИС ТО), осуществляющие эксплуатацию РИС ТО, а также имеющие подключение к РИС ТО.

3. Действие настоящего Регламента не распространяется на порядок организации доступа к информации, содержащей сведения, составляющие государственную тайну.

4. Исполнение требований настоящего Регламента является элементом служебной дисциплины и обязательно для всех пользователей РИС ТО в части, их касающейся.

II. Термины и определения

Авторизация – предоставление пользователю доступа к защищаемому информационному ресурсу в соответствии с заранее установленным ему уровнем доступа.

Аутентификатор – 1) отличительный, никому более не присущий признак пользователя (например, пароль, сертификат или биометрические данные); 2) техническое устройство индивидуального использования, служащее для хранения и ввода в персональный компьютер (далее – ПК) отличительного признака пользователя (например, токен, устройство iButton и др.).

Аутентификация – процесс подтверждения личности пользователя путем проверки (соотнесения) предъявляемых им идентификатора и аутентификатора(-ов).

Двухфакторная аутентификация – аутентификация, в процессе которой используются аутентификационные факторы нескольких типов (например, пользователь должен предоставить USB-ключ или смарт-карту и ввести пароль).

Защита информации – деятельность по обеспечению безопасности информации.

Идентификатор – имя пользователя.

Компрометация аутентификатора – хищение, утрата, разглашение, несанкционированное копирование и другие инциденты безопасности, в результате которых возникают сомнения в сохранении тайны аутентификатора.

Парольная документация – документы, содержащие парольную информацию и предназначенные для обеспечения функционирования системы аутентификации пользователей.

Пользователь – субъект доступа, обращающийся к информационному ресурсу в целях получения информации или воздействия на нее.

Уровень доступа – совокупность прав доступа пользователя к информационным ресурсам РИС ТО.

III. Авторизация пользователей РИС ТО

5. Заявка на предоставление пользователю доступа к информационным ресурсам РИС ТО (приложение № 1) оформляется за подписью руководителя организации, сотрудником которой является пользователь, и направляется в адрес оператора соответствующей РИС ТО посредством региональной системы электронного документооборота Тульской области (далее – РСЭД ТО)[1] с указанием реквизитов приказа о назначении пользователя (или с приложением копии выписки из приказа). Оператор[2] рассматривает данную заявку и при принятии положительного решения обращается в государственное автономное учреждение Тульской области «Центр информационных технологий» (далее – ГАУ ТО «ЦИТ») для настройки доступа к соответствующим ресурсам РИС ТО.

Организации, являющиеся операторами, определены в положениях о соответствующих РИС ТО.

6. При необходимости предоставления постоянного доступа к РИС ТО для сотрудников тех УИВ РИС ТО, которые не являются государственным органом и органом местного самоуправления Тульской

---

[1] В случае отсутствия доступа к РСЭД ТО заявка может оформляться на бумажном носителе.

[2] Для предоставления доступа к региональной информационной системе правительства Тульской области заявка направляется в государственное автономное учреждение Тульской области «Центр информационных технологий».

области и не включены в перечень государственных учреждений Тульской области, имеющих право доступа к РИС ТО (далее – Перечень) (приложение № 2), и при необходимости эксплуатации ими автоматизированных рабочих мест (далее – АРМ), обслуживаемых ГАУ ТО «ЦИТ», администратором безопасности (далее – АБ)[3] УИВ РИС ТО заполняется специальная форма согласования предоставления прав доступа пользователю (приложение № 3).

В данную форму вносится следующая информация:

– перечень информационных ресурсов, указанных в заявке (приложение № 1), и обоснование предоставления доступа к ним;

– принадлежность ПК (организация, являющаяся балансодержателем);

– сведения об отсутствии на АРМ контрафактного (нелицензионного) и не отвечающего «Требованиям к перечню и порядку использования программного обеспечения в аппарате правительства Тульской области, органах исполнительной власти Тульской области и их подведомственных учреждениях», утвержденным министерством по информатизации, связи и вопросам открытого управления Тульской области (далее – Требования), программного обеспечения (далее – ПО), в том числе операционной системы (далее – ОС);

– сведения об установленных и настроенных средствах защиты информации (далее – СЗИ), прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации (средство антивирусной защиты информации (далее – АВЗ), средство межсетевого экранирования (далее – МЭ), СЗИ от несанкционированного доступа (далее – НСД)).

При наличии на АРМ нелицензионного ПО или ПО, не удовлетворяющего Требованиям, а также в случае отсутствия на АРМ установленных и настроенных СЗИ, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, АБ УИВ РИС ТО инициирует работы по устранению выявленных несоответствий, по завершении которых вносит собранные сведения в вышеуказанную форму (приложение № 3) и передает ее на согласование руководителю государственного органа Тульской области, осуществляющего правомочия обладателя информации соответствующей РИС ТО (далее – Руководитель).

---

[3] АБ – лицо, ответственное за защиту информации и осуществляющее мероприятия по обеспечению безопасности информации.

АБ может быть назначен из числа сотрудников УИВ РИС ТО либо из числа сотрудников организации, лицензиата Федеральной службы безопасности Российской Федерации, на основании заключенных договоров.

Доступ к указанным в заявке информационным ресурсам соответствующей РИС ТО предоставляется после принятия Руководителем положительного решения.

7. В случае необходимости предоставления временного доступа к РИС ТО для лиц, не являющихся служащими или работниками УИВ РИС ТО (практиканты, стажеры и т. п.), в заявке (приложение № 1) должен быть указан срок, в течение которого будет действовать временная учетная запись. Такой пользователь должен подписать обязательство о неразглашении информации ограниченного доступа (приложение № 4).

8. Заявка на предоставление доступа пользователям из числа работников ГАУ ТО «ЦИТ» осуществляется особым порядком – путем обращения работника отдела кадрового и документационного обеспечения управления по обеспечению деятельности и развитию ГАУ ТО «ЦИТ» в службу поддержки пользователей ГАУ ТО «ЦИТ».

9. Доступ к информационным ресурсам РИС ТО, указанным в заявке, реализуется в течение 3 рабочих дней с даты ее поступления в ГАУ ТО «ЦИТ» либо с даты получения ГАУ ТО «ЦИТ» формы согласования предоставления прав доступа пользователю (приложение № 3), подписанной Руководителем (в соответствии с п. 6). Количество учетных записей пользователей, предоставленных для УИВ РИС ТО, не должно превышать количество учетных записей, предусмотренное в Договоре SLA.

10. Учетные записи нового пользователя для доступа к ресурсам РИС ТО создаются и передаются ему соответствующим АБ (при наличии требуемых прав) и (или) системными администраторами РИС ТО[4].

11. Доступ к защищаемому информационному ресурсу обеспечивается минимально необходимому и достаточному для выполнения служебных задач числу сотрудников, определяемому таблицей допуска к информационным ресурсам РИС ТО (далее – таблица допуска) (приложение № 5).

12. Таблицей допуска определяются разрешенные режимы работы пользователей и уровни их доступа к информационным ресурсам РИС ТО.

13. Пользователям предоставляются минимально необходимые и достаточные для исполнения служебных обязанностей права доступа к информационным ресурсам РИС ТО.

14. Авторизация пользователей РИС ТО происходит на основании положительных результатов аутентификации. Не допускается авторизация неидентифицированных пользователей.

---

[4] Системный администратор РИС ТО – лицо, ответственное за управление (администрирование) РИС ТО, виртуальной и сетевой инфраструктурой правительства Тульской области. К системным администраторам РИС ТО относятся в том числе и специалисты службы поддержки пользователей ГАУ ТО «ЦИТ».

15. В качестве усиления мер по идентификации и аутентификации пользователей может применяться двухфакторная аутентификация пользователей как в случае локального, так и для удаленного доступа к ресурсам РИС ТО.

IV. Принцип авторизации пользователей

16. Для доступа к информационным ресурсам РИС ТО запрещается использовать обезличенные учетные записи или в качестве идентификатора использовать обезличенные символьные последовательности.

17. В качестве аутентификатора пользователя могут использоваться пароль (кодовое слово), который вводится в ПК с клавиатуры, сертификат или биометрические данные, которые вводятся в ПК при помощи специального устройства аутентификации по биометрическим данным или считываются из специализированного электронного носителя индивидуального пользования, предназначенного для хранения аутентификатора (например, токена или устройства iButton).

18. Запрещается передача своих личных идентификаторов и аутентификаторов другим пользователям. Пользователь несет персональную ответственность за компрометацию своих аутентификаторов.

19. В случае неуспешных попыток аутентификации восемь раз подряд в течение 5 минут производится блокировка учетной записи пользователя на 30 минут.

20. Хранение пользователем парольной документации, в том числе значений своих паролей на бумажном носителе, и электронного носителя аутентификатора допускается только в личном, опечатанном пользователем (владельцем пароля) хранилище либо в сейфе у АБ или руководителя подразделения в опечатанном личной печатью (штампом организации) конверте.

21. Аутентификация пользователя производится посредством соотнесения предъявляемого им аутентификатора и предъявленного идентификатора (имени пользователя).

22. Аутентификация пользователя РИС ТО выполняется при:

– включении ПК[5] (при необходимости);

– входе в защищенную сеть;

– обращении к ресурсам.

23. Авторизация пользователей производится при положительном результате аутентификации.

---

[5] Аутентификация при включении ПК может осуществляться с использованием сертифицированных программных и программно-аппаратных средств защиты от несанкционированного доступа.

24. При авторизации пользователей должны обеспечиваться учет перечня информационных ресурсов РИС ТО и учет прав доступа пользователей. Таблицы допуска должны быть своевременно актуализированы.

25. Указанные мероприятия должны проводиться по мере необходимости, но не реже одного раза в год.

26. Таблицы допуска с указанием разрешенных режимов работы и уровней доступа разрабатываются силами АБ соответствующего УИВ РИС ТО, утверждаются оператором соответствующей РИС ТО и хранятся у АБ в сейфе или металлическом шкафу, исключающем НСД к ним.

27. Таблицы допуска к нескольким информационным ресурсам РИС ТО оформляются в виде единого документа при условии указания в таком документе сотрудников одной организации.

28. Таблица допуска должна иметь на титульном листе ограничительную пометку «Для служебного пользования» и быть оформлена как документ для служебного пользования.

29. Методическая помощь по уточнению прав доступа для конкретного пользователя осуществляется системными администраторами РИС ТО.

V. Требования к идентификаторам и аутентификаторам

30. Структура идентификаторов пользователей определяется возможностями ПО применяемых ОС и приложений, электронных носителей аутентификаторов и средств аутентификации.

31. Пароли учетных записей пользователей должны выбираться с учетом следующих требований:

– длина пароля должна быть не менее 8 символов;

– в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и (или) специальные символы (@, #, $, &, *, % и т. п.);

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций и т. д.), а также общепринятые сокращения и термины (user, qwerty, password, 123456 и т. п.);

– при смене пароля новое значение должно отличаться от предыдущих, использованных ранее;

– при создании паролей учетных записей пользователей возможно использование специализированного ПО для генерации сложных для подбора, но легко запоминаемых паролей.

32. Смена аутентификаторов, вводимых с клавиатуры, выполняется не реже, чем через 90 суток. Смена аутентификаторов, хранение и предъявление

которых системе аутентификации осуществляется посредством специализированного электронного носителя, производится не реже, чем один раз в год.

33. PIN-код электронного носителя аутентификатора устанавливается (изменяется) его пользователем. Пользователь обязан сохранять конфиденциальность по отношению к действующему PIN-коду используемого электронного носителя аутентификатора.

34. PIN-код электронного носителя аутентификатора должен соответствовать требованиям стойкости, рекомендованным его эксплуатационной документацией.

VI. Порядок назначения паролей

35. На основании таблицы допуска в соответствии с предоставленным уровнем доступа АБ или системный администратор РИС ТО (с использованием специализированных или встроенных средств защиты) осуществляет настройку системы разграничения доступа (аутентификации пользователей) путем назначения паролей для первого входа в систему или выпуска (при необходимости) сертификатов.

36. Установка/изменение паролей после первого входа, если это позволяют встроенные программные средства РИС ТО, производится пользователями самостоятельно, в соответствии с правилами и сроками, установленными п. V настоящего Регламента.

37. Контроль за выполнением мероприятий по организации парольной защиты в РИС ТО осуществляется отделом информационной безопасности департамента информационной безопасности и информатизации министерства по информатизации, связи и вопросам открытого управления Тульской области.

VII. Смена аутентификаторов при кадровых изменениях

38. В случае прекращения служебного контракта (трудового договора) с государственным гражданским служащим (работником), предоставления отпуска по уходу за ребенком, а также при необходимости и при кадровых перестановках, на основании приказов кадровых служб УИВ РИС ТО, размещаемых и рассылаемых в РСЭД ТО в адрес ГАУ ТО «ЦИТ» или направляемых посредством защищенной электронной почты ViPNet «Деловая почта», АБ соответствующего УИВ РИС ТО и (или) системные администраторы РИС ТО вносят изменения в учетные записи.

Также при возникновении вышеуказанных кадровых изменений УИВ РИС ТО может предоставлять соответствующую информацию в ГАУ ТО «ЦИТ» посредством оформления заявки в РСЭД ТО (приложение № 1) или, обратившись в службу поддержки пользователей ГАУ ТО «ЦИТ», оставить заявку на блокирование доступа к РИС ТО (с перечислением конкретных ресурсов) в день увольнения (кадрового перевода) пользователя.

39. На основании приказов о предоставлении ежегодного оплачиваемого отпуска учетные записи пользователей государственных органов Тульской области частично блокируются (ограничивается доступ к РИС ТО, за исключением служебной электронной почты и средства обмена мгновенными сообщениями) на весь период отпуска. Частичная блокировка учетной записи на период ежегодного оплачиваемого отпуска не фиксируется в таблицах допуска.

40. Учетные записи увольняемых (переводимых) пользователей блокируются в день увольнения (кадрового перевода в другую организацию).

41. При увольнении или кадровом переводе АБ или системного администратора РИС ТО замене подлежат все установленные им пароли и доступная ему парольная документация.

VIII. Действия при компрометации аутентификатора

42. Под компрометацией аутентификатора понимаются:

– утеря (хищение) аутентификатора, в том числе с последующим его обнаружением;

– увольнение сотрудника, имевшего доступ к аутентификационной информации;

– передача паролей по незащищенным линиям связи;

– нарушение правил хранения аутентификатора;

– несанкционированное или безучетное копирование аутентификатора;

– нарушение целостности печати на сейфе с аутентификатором;

– вскрытие фактов утечки (искажения или изменения) передаваемой информации;

– все случаи, когда нельзя достоверно установить, что произошло с аутентификатором.

43. При выявлении факта компрометации или подозрении на компрометацию аутентификатора пользователь незамедлительно обязан сообщить непосредственному руководителю и обратиться к АБ.

44. В случае выявления факта компрометации пользователем аутентификатора АБ обязан немедленно заблокировать

скомпрометированную учетную запись либо в случае отсутствия возможности самостоятельной блокировки обратиться в службу поддержки пользователей ГАУ ТО «ЦИТ».

О выявленном факте АБ обязан доложить своему руководителю, а также оператору соответствующей РИС ТО.

45. По факту компрометации АБ проводит расследование инцидента информационной безопасности, к которому могут привлекаться сотрудники оператора, сотрудники ГАУ ТО «ЦИТ», а также сотрудники организации, в которой имел место факт компрометации.

Результаты расследования оформляются в соответствующем акте за подписью АБ и его непосредственного руководителя с последующим направлением копии указанного акта в адрес УИВ РИС ТО, в котором зафиксирован инцидент безопасности, оператору РИС ТО и в министерство по информатизации, связи и вопросам открытого управления Тульской области для принятия соответствующих мер реагирования по устранению выявленного инцидента безопасности и предотвращению подобных инцидентов в будущем.

46. Разблокировка учетной записи с принудительной сменой всех скомпрометированных паролей (PIN-кода электронного идентификатора) и выдача пользователю нового аутентификатора производится по решению руководителя УИВ РИС ТО и по согласованию с отделом информационной безопасности департамента информационной безопасности и информатизации министерства по информатизации, связи и вопросам открытого управления Тульской области.

IX. Требования к средствам выработки паролей

47. Пароли вырабатываются АБ или системными администраторами РИС ТО.

48. Для выработки паролей используется специализированное ПО, установленное на ПК, оборудованном системой защиты информации от НСД, которой должны реализовываться следующие функции:

– аутентификация пользователя при включении ПК;

– проверка целостности аппаратного и программного обеспечения ПК;

– автоматическая регистрация действий пользователя в электронном журнале;

– блокирование работы ПК при фиксировании предъявления восьми подряд неверных аутентификаторов.

49. При использовании индивидуальных электронных аутентификаторов (ключей) средства формирования паролей или

сертификатов должны соответствовать требованиям технической документации на эти устройства и использующиеся ОС.

X. Ответственность

50. АБ, системные администраторы и пользователи РИС ТО несут персональную ответственность за соблюдение требований настоящего Регламента.

51. АБ, системные администраторы и пользователи РИС ТО могут быть привлечены к дисциплинарной, а в соответствующих случаях – к материальной и уголовной ответственности в порядке, установленном законодательством Российской Федерации.

Министр по информатизации, связи и вопросам открытого управления Тульской области **Я.Ю. Раков**

Приложение № 1
к Регламенту по организации парольной защиты
в региональных информационных системах
Тульской области

Форма заявки на изменение прав доступа к РИС ТО

Руководителю организации
– оператора РИС ТО
Ф.И.О.

ЗАЯВКА

В связи с _____
(назначением, переводом, изменением должностных обязанностей,

_____
выходом из отпуска по уходу за ребенком, увольнением, прочее)

на основании приказа _____
(реквизиты кадрового приказа)

_____
(должность и подразделение сотрудника)

_____
(Ф.И.О. сотрудника)

прошу _____ доступ указанному сотруднику
(предоставить, изменить, ограничить)

к следующим информационным ресурсам _____
(наименование конкретной РИС ТО)

_____ на срок с «___» _____ 201_ г. до «___» _____ 201_ г.:
(даты указываются при предоставлении временного доступа)

1. _____
(наименование информационного ресурса и при необходимости тип прав доступа)
2. _____
(наименование информационного ресурса и при необходимости тип прав доступа)
3. _____
(наименование информационного ресурса и при необходимости тип прав доступа)

…

_____ _____/_____/
(должность руководителя организации) (подпись) (Ф.И.О.)

«___» _____ 201_ г.
(дата)

Приложение № 2
к Регламенту по организации парольной защиты
в региональных информационных системах
Тульской области

Перечень государственных учреждений Тульской области, имеющих право доступа к региональным информационным системам Тульской области

№ п/п	Наименование учреждения	Курирующий государственный орган
1	Государственное автономное учреждений Тульской области «Центр информационных технологий»	Министерство по информатизации, связи и вопросам открытого управления Тульской области
2.	Государственное бюджетное учреждение Тульской области «Многофункциональный центр предоставления государственных и муниципальных услуг»	Министерство по информатизации, связи и вопросам открытого управления Тульской области
3.	Государственное казенное учреждение Тульской области «Центр организации закупок»	Министерство финансов Тульской области
4.	Государственное казенное учреждение Тульской области «Централизованная бухгалтерия органов исполнительной власти Тульской области»	Министерство финансов Тульской области
5.	Государственное казенное учреждение Тульской области «Централизованная бухгалтерия министерства образования Тульской области»	Министерство образования Тульской области
6.	Государственное казенное учреждение Тульской области «Экспертиза»	Комитет Тульской области по тарифам
7.	Государственное образовательное учреждение дополнительного профессионального образования Тульской области «Институт повышения квалификации и профессиональной переподготовки работников»	Министерство образования Тульской области
8.	Государственное учреждение здравоохранения Тульской области «Тульский областной медицинский информационно-аналитический центр»	Министерство здравоохранения Тульской области
9.	Государственное учреждение культуры Тульской области «Центр технического надзора и мониторинга деятельности учреждений культуры Тульской области»	Министерство культуры Тульской области
10.	Государственное учреждение Тульской области «Аппарат Общественной палаты Тульской области»	Министерство труда и социальной защиты Тульской области
11.	Государственное учреждение Тульской области «Областное бюро технической инвентаризации»	Министерство имущественных и земельных отношений Тульской области

№ п/п	Наименование учреждения	Курирующий государственный орган
12.	Государственное учреждение Тульской области «Представительство правительства Тульской области»	Управление делами аппарата правительства Тульской области
13.	Государственное учреждение Тульской области «Сервис»	Управление делами аппарата правительства Тульской области
14.	Государственное учреждение Тульской области «Центр технического надзора, эксплуатации зданий и сооружений учреждений образования»	Министерство образования Тульской области
15.	Государственное учреждение Тульской области «Центр технического надзора, эксплуатации зданий и сооружений учреждений здравоохранения»	Министерство здравоохранения Тульской области
16.	Специализированное государственное учреждение при правительстве Тульской области «Фонд имущества Тульской области»	Министерство имущественных и земельных отношений Тульской области

Приложение № 3
к Регламенту по организации парольной защиты
в региональных информационных системах
Тульской области

Форма согласования предоставления прав доступа пользователю

Согласовано

Должность руководителя соответствующего государственного органа Тульской области, осуществляющего правомочия обладателя информации конкретной РИС ТО

_____ Ф.И.О.

«_____»_____201____г.

Курирующий государственный орган	**Наименование учреждения**		**Статус рабочего места (существующее / дополнительное)**	
ФИО	**Должность**	**Адрес**	**Кабинет**	**Телефон**

Запрос на доступ к следующим информационным ресурсам:	**Обоснование необходимости доступа**	**Отметка о разрешении доступа**

ПК			
ОС (лицензия)			
ПО			
СЗИ	АВЗ		
	МЭ		
	СЗИ от НСД		

Приложение № 4
к Регламенту по организации парольной защиты
в региональных информационных системах
Тульской области

ФОРМА

ОБЯЗАТЕЛЬСТВО
о неразглашении информации ограниченного доступа

Я, _____,
(фамилия, имя, отчество)

_____,
(адрес)

паспорт _____, выдан _____, _____
(серия, номер) (дата) (кем выдан)

_____

предупрежден(-а), что при _____
(прохождении мною практики /

_____
прохождении мною стажировки / исполнении служебных обязанностей / иное)
в случае моего доступа к информации ограниченного доступа (в том числе к персональным данным) добровольно принимаю на себя обязательства:

1. Не разглашать третьим лицам ставшую мне известной информацию ограниченного доступа.

2. В случае попытки третьих лиц получить от меня информацию ограниченного доступа сообщать об этом непосредственному руководителю или администратору безопасности _____

_____.
(наименование организации, предоставившей доступ к информационной системе)

3. Не использовать информацию ограниченного доступа в личных целях.

4. Выполнять требования законодательства Российской Федерации, нормативных правовых актов правительства Тульской области, министерства по информатизации, связи и вопросам открытого управления Тульской области и локальных актов _____

_____,
(наименование оператора соответствующей РИС ТО)

регламентирующих вопросы обработки и защиты информации ограниченного доступа.

Я предупрежден(-а), что лица, виновные в нарушении законодательства Российской Федерации в сфере защиты информации ограниченного доступа, привлекаются к дисциплинарной, гражданско-правовой, административной или уголовной ответственности.

Персональные данные, содержащиеся в настоящем документе, будут обрабатываться _____,
(наименование организации, предоставившей доступ к информационной системе)

_____,
(адрес организации, предоставившей доступ к информационной системе)

смешанным способом с целью _____
(учета проходящих практику лиц / учета проходящих стажировку лиц /

_____
учета лиц, допущенных к обработке информации ограниченного доступа при исполнении служебных обязанностей / иное)

в течение 3 лет. Настоящий документ заполняется субъектом собственноручно. Перечень действий, осуществляемых с персональными данными: получение (сбор), запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача в министерство по информатизации, связи и вопросам открытого управления Тульской области и государственное автономное учреждение Тульской области «Центр информационных технологий» (адрес указанных операторов персональных данных: 300041, г. Тула, пр. Ленина, д. 2), блокирование, удаление, уничтожение персональных данных.

_____ «____»_____ _____ г.
(подпись) (дата заполнения)

Приложение № 5
к Регламенту по организации парольной защиты
в региональных информационных системах
Тульской области

Форма таблицы допуска пользователей к РИС ТО

УТВЕРЖДАЮ
Должность руководителя организации –
оператора соответствующей РИС ТО
_____/_____/
(подпись) (Ф.И.О)
«___» _____ 201_ г.
(дата)

Таблица допуска к информационным ресурсам *наименование региональной информационной системы Тульской области*

государственных гражданских служащих и (или) работников
наименование организации

наименование информационного ресурса

№ п/п	Должность (с указанием органа власти / учреждения / организации)	Фамилия, имя, отчество	Режим функционирования и уровень доступа*	Режим функционирования и уровень доступа	Режим функционирования и уровень доступа	Режим функционирования и уровень доступа
1	**2**	**3**	**4**	**5**	**…**	**N***
1.						
2.						
3.						
…						

* Количество и наименования граф разрабатываются с учетом специфики каждого информационного ресурса