ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ТВЕРСКОЙ ОБЛАСТИ
«ЦЕНТР ИНФОРМАТИЗАЦИИ ОБРАЗОВАНИЯ ТВЕРСКОЙ ОБЛАСТИ»

ПРИКАЗ

05.12.2017 **г. Тверь** **№ 12**

Об утверждении Политики информационной безопасности ГБУ «ТверьИнформОбр»

В целях обеспечения защиты информации, обрабатываемой в информационных системах ГБУ «ТверьИнформОбр», в соответствии с распоряжением Правительства Тверской области от 12.10.2017 № 345-рп и с постановлением Правительства Тверской области «Об утверждении Политики информационной безопасности исполнительных органов государственной власти Тверской области, государственных учреждений Тверской области и государственных унитарных предприятий Тверской области»

ПРИКАЗЫВАЮ:

1. Утвердить Политику информационной безопасности Государственного бюджетного учреждения Тверской области «Центр информатизации образования Тверской области» (далее – Политика) (прилагается).
2. Ответственность за выполнение положений Политики в ГБУ «ТверьИнформОбр» возложить на И.о. заместителя директора ГБУ «ТверьИнформОбр» А.В. Строганова.
3. Контроль за исполнением настоящего приказа оставляю за собой.
4. Настоящий приказ вступает в силу со дня его подписания.

И.о. директора
ГБУ ТверьИнформОбр» **М.В. Пищулин**

С приказом ознакомлен:
А.В. Строганов _____ 05.12.2017

Приложение
к приказу ГБУ «ТверьИнформОбр»
от 05.12.2017 № 12

Политика
Информационной безопасности
Государственного бюджетного учреждения Тверской области
«Центр информатизации образования
Тверской области»

Раздел I
Общие положения

1. Политика информационной безопасности Государственного бюджетного учреждения Тверской области «Центр информатизации образования Тверской области» (далее – Учреждение) представляет собой совокупность правил, процедур, практических приемов и общих принципов защиты информации, определяющих особенности эксплуатации информационных систем Учреждения (далее – информационные системы), которыми Министерство руководствуются при создании и эксплуатации информационных систем.

2. Целями реализации Политики являются минимизация ущерба от реализации угроз безопасности информации, повышение деловой репутации и корпоративной культуры сотрудников Учреждения при использовании ими информационных технологий.

3. В ходе реализации Политики Учреждения руководствуются следующими принципами:

а) принцип законности, в соответствии с которым все организационные мероприятия должны соответствовать федеральному законодательству и законодательству Тверской области в сфере защиты информации;

б) принцип комплексного подхода к обеспечению информационной безопасности, при котором обеспечить ее необходимый уровень возможно только путем совокупности организационных мероприятий и технических мер, включающих в себя физическую охрану носителей информации, использование категорий информации для обозначения уровня конфиденциальности документов, подбор и подготовку кадров в сфере информационной безопасности, использование технических средств защиты информации, обучение сотрудников, расследование инцидентов информационной безопасности;

в) принцип непрерывности, в соответствии с которым обеспечение информационной безопасности является постоянным процессом, который состоит из регулярных проверок актуальности угроз информационной безопасности, проверок адекватности мер защиты существующим угрозам

информационной безопасности, регулярной модернизации средств защиты информации, своевременного повышения квалификации специалистов, иных мероприятий;

г) принцип специализации, который подразумевает возможность привлекать для проектирования и внедрения специальных программных и технических средств защиты специалистов, имеющих соответствующий опыт, или организации, имеющие лицензию на соответствующий вид деятельности;

д) принцип экономической целесообразности, в соответствии с которым при реализации мероприятий по обеспечению информационной безопасности расходы областного бюджета Тверской области на эти цели соизмеряются с вероятным ущербом от реализации угроз информационной безопасности;

е) принцип своевременности, подразумевающий упреждающий характер мероприятий по обеспечению информационной безопасности, прогнозирование появления угроз информационной безопасности на этапе проектирования информационных систем Тверской области и осуществление модернизации средств защиты информации при внесении изменений в существующие информационные системы Тверской области;

ж) принцип взаимодействия, предполагающий взаимодействие и распределение зон ответственности между ИОГВ Тверской области, государственными учреждениями, унитарными предприятиями Тверской области при обеспечении информационной безопасности, а также организацию сотрудничества в этой сфере со сторонними экспертами и организациями – лицензиатами, а также федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации.

4. В целях реализации требований Политики в Учреждении назначается администратор информационной безопасности из числа сотрудников Учреждения, ответственный за принятие организационных и технических мер по защите информации.

5. Для целей Политики применяются следующие термины:

а) администратор информационной безопасности – должностное лицо Учреждения, ответственное за соблюдение требований законодательства в сфере защиты информации;

б) вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы;

в) инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность Учреждения (утрата услуг, оборудования или устройств, системные сбои или перегрузки, ошибки пользователей, несоблюдение политики информационной безопасности, нарушение

физических мер защиты, неконтролируемые изменения информационных систем, сбои программного обеспечения и отказы технических средств, нарушение правил доступа);

г) лицензионное программное средство – программное средство, использование одной или нескольких копий которого осуществляется на основе лицензии – правового инструмента, определяющего использование и распространение программного средства, защищенного авторским правом;

д) масштаб информационной системы:

федеральный – если информационная система функционирует на территории Российской Федерации (в пределах федерального округа) и имеет сегменты (технические средства информационных систем) в субъектах Российской Федерации, муниципальных образованиях и (или) организациях;

региональный (межведомственный) – если информационная система функционирует на территории Тверской области и имеет сегменты (технические средства информационных систем) в одном или нескольких муниципальных образованиях Тверской области и (или) подведомственных и иных организациях Тверской области;

объектовый – если информационная система функционирует на объектах одного федерального органа исполнительной власти, ИОГВ Тверской области (государственного учреждения, унитарного предприятия Тверской области), муниципального образования Тверской области и (или) организации и не имеет сегментов (технических средств информационных систем) в территориальных органах, представительствах, филиалах, подведомственных и иных организациях;

е) несанкционированный доступ к информации – доступ к информации, нарушающий установленные правила ее получения;

ж) пользователь информационной системы (средства вычислительной техники) – лицо, участвующее в функционировании информационной системы (средства вычислительной техники) или использующее результаты ее функционирования;

з) программное обеспечение – совокупность программных средств и программных продуктов;

и) программное средство – объект, состоящий из программ, процедур, правил, а также, если предусмотрено, сопутствующих им документов и данных, относящихся к функционированию информационной системы;

к) программный продукт – программное средство, предназначенное для поставки, передачи, продажи пользователю;

л) средство криптографической защиты информации (далее также – СКЗИ) – аппаратные, программно-аппаратные и программные средства, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности;

м) средство вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем;

н) сервер – компьютер, выделенный из группы персональных компьютеров для выполнения какой-либо сервисной задачи без непосредственного участия человека;

о) спам – телематическое электронное сообщение, предназначенное неопределенному кругу лиц, доставленное абоненту и (или) пользователю без их предварительного согласия и не позволяющее определить отправителя этого сообщения, в том числе ввиду указания в нем несуществующего или фальсифицированного адреса отправителя;

п) учетная запись «Администратор» – учетная запись пользователя информационной системы, позволяющая вносить изменения в настройки информационной системы, затрагивающие всех пользователей информационной системы (изменение параметров безопасности, установка программного обеспечения, работа с любыми файлами в информационной системе, изменение параметров учетных записей других пользователей).

Раздел II
Классификация информационных систем Учреждения

6. Информационные системы Учреждения могут содержать общедоступную информацию и информацию ограниченного доступа.

7. В зависимости от категории информации, содержащейся в информационных системах, информационные системы подразделяются на следующие типы:

а) информационные системы, содержащие сведения, представляющие общедоступную информацию;

б) информационные системы, содержащие сведения, составляющие государственную тайну;

в) информационные системы, содержащие служебные сведения ограниченного доступа;

г) информационные системы персональных данных.

Раздел III
Инвентаризация информационных систем Учреждения

8. Инвентаризация информационных систем (далее – инвентаризация) проводится в Учреждении не реже одного раза в год.

Целью инвентаризации является получение полной и достоверной информации об объеме и составе информационных систем и их технических средств для обеспечения безопасности информации при их эксплуатации.

В перечень информационных систем, подлежащих инвентаризации, могут быть включены любые информационные системы, указанные в пункте 7 раздела II Политики, независимо от их местонахождения.

Основанием для проведения инвентаризации является приказ Учреждения.

9. Для проведения инвентаризации в Учреждении приказом Учреждения создается инвентаризационная комиссия. В приказе о создании

инвентаризационной комиссии устанавливаются сроки проведения инвентаризации, утверждаются руководителем, а также персональный состав инвентаризационной комиссии, в который могут быть включены:

а) руководителя Учреждения, ответственный за организацию защиты информации;

б) работник, осуществляющий бухгалтерский (бюджетный) учет;

в) администратор информационной безопасности.

10. Инвентаризация включает следующие мероприятия:

а) описание информационной системы, в котором отражаются границы информационной системы, размещение ее технических средств и поддерживающей инфраструктуры применительно к организационной структуре Учреждения, определяется масштаб информационной системы;

б) определение типа информационной системы в зависимости от категории, обрабатываемой в ней информации;

в) группировка по отдельным признакам (например, по тематикам) файлов, созданных пользователями, не отнесенных ни к одной из информационных систем, но представляющих информационную ценность для Учреждения;

г) определение порядка использования информационных систем, в ходе которого уточняется эксплуатируется ли указанная информационная система только в интересах Учреждения или же используется совместно с пользователями других ИОГВ Тверской области (государственных учреждений, унитарных предприятий Тверской области), указывается количество пользователей информационной системы, а также определяется должностное лицо, ответственное за ее эксплуатацию;

д) уточнение комплекса мероприятий по поддержанию, развитию, совершенствованию и защите информационных систем.

11. На основе данных, полученных по итогам инвентаризации, администратор информационной безопасности составляет перечень информационных систем Учреждения в соответствии с приложением 1 к Политике, а также составляет или уточняет перечень данных, подлежащих резервному копированию и хранению в Учреждении в соответствии с приложением 2 к Политике. Перечни информационных систем Учреждения передаются в исполнительный орган власти Тверской области, уполномоченный в сфере информационных технологий, для занесения в реестр информационных систем Тверской области.

Раздел IV
Управление доступом к информационным системам Учреждения

12. Основные правила и методы защиты информационных систем от несанкционированного доступа:

а) для управления доступом к информационным системам Учреждения вводится разрешительная система допуска пользователей (обслуживающего персонала) к информационным системам и связанным с их использованием, работам и документам;

б) для входа в информационную систему используется парольная аутентификация, при необходимости – другие способы аутентификации;

в) при любом оставлении сотрудником рабочего места средство вычислительной техники информационной системы должно блокироваться и требовать аутентификации для дальнейшего продолжения работы;

г) каждому сотруднику Учреждения, имеющему право доступа к информационной системе, присваивается отличная от других учетная запись пользователя;

д) каждый сотрудник при получении переданного ему пароля доступа к информационной системе или иных средств аутентификации информируется, что он предупрежден о необходимости сохранять полученный пароль в тайне, не передавать вверенный ему пароль или иные средства аутентификации третьим лицам, в том числе другим сотрудникам Учреждения.

13. Разрешительная система допуска пользователей (обслуживающего персонала) к информационным системам и связанным с их использованием работам и документам подразумевает:

а) вход в информационные системы с помощью учетной записи, относящейся к типу «Администратор», разрешен только лицам, уполномоченным на выполнение административных функций в информационных системах;

б) вход в информационные системы остальным пользователям разрешен только с использованием ограниченной учетной записи, позволяющей им обрабатывать информацию в данных информационных системах исключительно в рамках их компетенции для исполнения своих должностных обязанностей;

в) сотрудникам разрешено использовать только те учетные записи, которые присвоены им в порядке, определенном Политикой;

г) учетные записи уволенных сотрудников, а также любого сотрудника, который не осуществлял доступ к информационной системе в течение трех месяцев, должны быть заблокированы и/или удалены из информационной системы. Для возобновления доступа данный сотрудник должен вновь пройти процедуру получения прав доступа к информационной системе.

14. Настройки средств вычислительной техники информационных систем в штатном режиме должны предусматривать загрузку операционных систем только с жестких дисков и исключать загрузку операционных систем с других носителей.

15. Допуск всех сотрудников к работе с информационными системами осуществляется только после их ознакомления с Политикой.

16. О выявленных попытках несанкционированного доступа к информационным системам администратор информационной безопасности незамедлительно сообщает руководителю Учреждения.

Руководитель Учреждения по факту попытки несанкционированного доступа к информационным системам назначается служебная проверка.

Раздел V
Основные правила и методы предотвращения неавторизованного доступа к информации Учреждения с использованием парольной аутентификации

17. Пароли подразделяются на пароли пользователей информационной системы и пароли администраторов информационной безопасности и относятся к служебным сведениям ограниченного доступа.

18. При первоначальном предоставлении пользователю доступа к информационной системе или в случае утери пароля пользователем, администратор информационной безопасности выдает временный пароль, который требуется сменить при первом входе в информационную систему.

19. Пароли администратора информационной безопасности подлежат хранению в сейфе у администратора информационной безопасности в запечатанном конверте с указанием наименования информационной системы, должности, фамилии, инициалов должностного лица, ответственного за эксплуатацию информационной системы.

20. Порядок хранения и использования паролей определяет администратор информационной безопасности.

21. Пароль пользователя информационной системы должен отвечать следующим требованиям:

а) длина пароля должна быть не менее 8 символов;

б) пароль не должен содержать в себе имя учетной записи пользователя информационной системы;

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

г) при смене пароля новое значение должно отличаться от предыдущего не менее чем в 2 позициях;

д) пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, даты рождений и т.д.);

е) пароль должен изменяться не реже чем один раз в 6 месяцев;

ж) пароль должен быть уникальным по отношению к паролям других учетных записей данного пользователя.

22. Пароль администратора информационной безопасности должен отвечать следующим требованиям:

а) длина пароля должна быть не менее 12 символов;

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

в) при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

г) пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, даты рождений и т.д.);

д) пароль должен изменяться не реже чем один раз в 3 месяца;

е) пароль должен быть уникальным по отношению к паролям других учетных записей администратора информационной безопасности.

23. Запрещается сообщать пароль кому-либо, в том числе при помощи почтовых сообщений, через информационно-телекоммуникационную сеть Интернет (далее – ИТКС Интернет), каким-либо иным способом.

24. При компрометации пароля пользователь должен сообщить об этом администратору информационной безопасности и незамедлительно сменить пароль.

Раздел VI
Основные правила и методы организации антивирусной защиты информационных систем Учреждения

25. Организация антивирусной защиты в Учреждении, а также контроль за выполнением мероприятий по антивирусной защите возлагаются на администраторов информационной безопасности.

26. На администратора информационной безопасности возлагаются следующие функции:

а) организация выбора средств антивирусной защиты, приобретения, установки на объекты защиты, настройки и сопровождения;

б) организация и проведение технических мероприятий по антивирусной защите;

в) разработка документов, устанавливающих правила безопасной работы со средствами вычислительной техники и регламентирующих действия пользователей в ситуациях, связанных с действием вредоносных программ.

27. К объектам антивирусной защиты относятся информация, содержащаяся в информационной системе, технические средства информационных систем (в том числе средства вычислительной техники), и предоставляемые ими сервисы (почта и т.д.), машинные носители информации, входящие в состав информационных систем или временно подключаемые к ним, средства и системы связи и передачи данных, общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

28. К средствам антивирусной защиты относятся программы, предназначенные для обнаружения и уничтожения вредоносных программ, а также ликвидации последствий от их воздействий.

29. Для антивирусной защиты информационных систем Учреждения используются официально приобретенные средства антивирусной защиты, сведения о которых содержатся в Государственном реестре сертифицированных средств защиты информации федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, и (или) федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности.

30. Рекомендуется использовать средства антивирусной защиты с возможностью централизованного управления и автоматической установкой обновлений антивирусного программного обеспечения и баз данных признаков вредоносных программ.

31. Для периодических проверок объектов антивирусной защиты рекомендуется использовать средства антивирусной защиты различных производителей.

32. Не допускается подключение и эксплуатация средств вычислительной техники в информационных системах без установленных и надлежащим образом настроенных активных и актуальных средств антивирусной защиты.

33. Пользователям информационных систем запрещается предпринимать попытки отключения, изменения настроек и влияния на работу эксплуатируемых средств антивирусной защиты.

34. При возникновении подозрения о наличии на средстве вычислительной техники вредоносных программ (нетипичная работа программного обеспечения, появление графических и звуковых эффектов, искажений данных, исчезновение (несанкционированное уничтожение) файлов, регулярное появление сообщений о системных ошибках и т.п.) пользователи информационных систем самостоятельно или вместе с администратором информационной безопасности проводят внеочередной антивирусный контроль средства вычислительной техники.

35. В случае обнаружения вредоносных программ пользователи информационных систем обязаны:

а) приостановить работу;

б) немедленно поставить в известность об этом администратора информационной безопасности и/или сотрудника подразделения по информационной безопасности, владельца зараженных файлов (ресурсов), а также других сотрудников, использующих эти файлы в работе;

в) совместно с владельцем зараженных файлов (ресурсов) провести анализ необходимости дальнейшего их использования;

г) провести лечение или уничтожение зараженных файлов.

36. В случае обнаружения вредоносных программ администратор информационной безопасности организует внеочередной антивирусный контроль всех средств вычислительной техники информационной системы, в которой обнаружена вредоносная программа.

37. Все файлы, полученные из ИТКС Интернет посредством электронной почты, а также копируемые на средства вычислительной техники с любых внешних носителей информации подлежат обязательной проверке средствами антивирусной защиты.

Раздел VII
Основные правила и методы организации резервного копирования в Учреждении

38. Ответственным за проведение резервного копирования, хранение резервных копий, а также восстановление информации является администратор информационной безопасности.

39. Администратор информационной безопасности в зависимости от функциональных особенностей эксплуатируемых информационных систем определяет перечень данных, подлежащих резервному копированию и хранению, в соответствии с приложением 2 к Политике, расписание резервного копирования в соответствии с приложением 3 к Политике и утверждает их у руководителя Учреждения.

40. Резервному копированию подлежит информация следующих основных категорий:

персональная информация пользователей (личные каталоги на файловых серверах);

групповая информация пользователей (общие каталоги подразделений);

информация, необходимая для восстановления серверов и систем управления базами данных;

персональные профили пользователей сети;

рабочие копии установочных компонент программного обеспечения вычислительных средств информационных систем Учреждения;

регистрационная информация подсистем информационной безопасности информационных систем Учреждения.

41. Для организации системы резервного копирования используются стандартные программные средства операционной системы либо специализированные лицензионные программные средства резервного копирования.

42. Средства резервного копирования должны обеспечивать производительность, достаточную для сохранения копируемой информации.

43. Информация с носителей, которые перестают использоваться в системе резервного копирования, стирается без возможности восстановления данных.

44. Хранение съемных носителей с резервными копиями осуществляется в отдельных запираемых сейфах, доступ к которым имеет только администратор информационной безопасности.

45. Все процедуры по загрузке, выгрузке носителей, на которые производится резервное копирование, а также любое перемещение съемных

носителей осуществляются администратором информационной безопасности.

46. Основанием для инициирования процедуры восстановления служит полная или частичная утрата информации вследствие сбоев оборудования, программного обеспечения в критических и кризисных ситуациях. Восстановление данных производится администратором информационной безопасности.

47. О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, администратор информационной безопасности сообщает руководителю Учреждения служебной запиской в течение рабочего дня после обнаружения указанного события.

48. Руководителем Учреждения по факту попытки несанкционированного доступа к резервируемой информации назначается служебная проверка.

49. Контроль результатов резервного копирования осуществляется администратором информационной безопасности. В случае обнаружения ошибки резервного копирования или выхода из строя системы резервного копирования администратор информационной безопасности выполняет повторное копирование информации вручную в максимально сжатые сроки, не нарушая технологические процессы обработки информации пользователями.

Раздел VIII
Порядок работы с электронной почтой в Учреждении

50. Электронная почта в Учреждении должна использоваться только в служебных целях.

51. При работе с электронной почтой Учреждения запрещается:

а) использовать адрес служебной электронный почты в личных целях;

б) публиковать свой адрес служебной электронный почты либо адреса других сотрудников на общедоступных интернет-ресурсах (форумы, конференции и т.п.) без предварительного согласования с руководителем Учреждения;

в) отправлять сообщения с вложенными файлами, общий размер которых превышает максимально допустимый;

г) открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами;

д) осуществлять массовую рассылку почтовых сообщений (более 43) внешним адресатам, если это не обусловлено служебной необходимостью;

е) осуществлять рассылку материалов, содержащих вредоносные программы, или файлы, предназначенные для нарушения, уничтожения либо ограничения функциональности электронного оборудования или программного обеспечения, для осуществления несанкционированного

доступа, а также серийные номера к коммерческим программным продуктам и программное обеспечение для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в ИТКС Интернет, а также ссылки на вышеуказанную информацию;

ж) распространять защищаемые авторскими правами материалы, затрагивающие какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и (или) авторские и смежные с ними права третьей стороны;

з) распространять информацию, содержание и направленность которой запрещены законодательством Российской Федерации, 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.;

и) осуществлять отправку сообщений электронной почты с чужого почтового ящика или от чужого имени;

к) распространять посредством сообщений электронной почты информацию, содержащую персональные данные, служебные сведения ограниченного доступа, сведения, относящиеся к государственной тайне.

Раздел IX
Порядок использования ИТКС Интернет в Учреждении

52. Доступ к ИТКС Интернет в Учреждении может предоставляться сотрудникам в целях выполнения ими своих служебных обязанностей.

53. Подключение средств вычислительной техники к ИТКС Интернет выполняется администратором информационной безопасности.

54. Средства вычислительной техники, используемые для обработки сведений, составляющих государственную тайну, не могут быть подключены к ИТКС Интернет.

55. При использовании ИТКС Интернет сотрудникам Учреждения запрещено:

а) использовать предоставленный доступ к ИТКС Интернет в личных целях;

б) использовать специализированные аппаратные и программные средства, позволяющие сотрудникам получить несанкционированный доступ к ИТКС Интернет;

в) совершать действия, направленные на нарушение функционирования элементов информационных систем;

г) публиковать, загружать и распространять материалы, содержащие:

информацию ограниченного доступа;

информацию, полностью или частично защищенную авторскими или другими правами, без разрешения владельца;

вредоносное программное обеспечение, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа, а также серийные номера к коммерческому программному обеспечению и программное обеспечение для их генерации, пароли и прочие средства для получения несанкционированного доступа к платным интернет-ресурсам, а также ссылки на вышеуказанную информацию;

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 и т.д.

56. При необходимости администратор информационной безопасности и/или сотрудник подразделения по информационной безопасности блокирует доступ к интернет-ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей.

57. При наличии технической возможности администратором информационной безопасности обеспечивается возможность протоколирования информации о посещаемых сотрудниками интернет-ресурсах для последующего анализа и по требованию руководителя Учреждения для контроля.

Раздел X
Использование программного обеспечения в информационных системах Учреждения

58. В Учреждении для выполнения возложенных на них функций разрешено применение ограниченного перечня коммерческого и свободного программного обеспечения.

59. Перечень программного обеспечения, разрешенного к использованию в Учреждении определяется администратором информационной безопасности. Разрешенное к использованию программное обеспечение заносится в реестр разрешенного к использованию программного обеспечения в соответствии с приложением 4 к Политике и утверждается руководителем Учреждения.

60. Перечень программного обеспечения, устанавливаемого на средство вычислительной техники, определяется администратором информационной безопасности исходя из должностных обязанностей пользователя, а также функций информационной системы Учреждения и заносится администратором информационной безопасности в паспорт средства вычислительной техники в соответствии с приложением 5 к Политике.

61. Установка и использование программного обеспечения, не занесенного в реестр разрешенного к использованию программного обеспечения, запрещается.

62. Все операции по установке, сопровождению, удалению программного обеспечения выполняются администратором информационной безопасности или техническими специалистами других организаций, привлекаемыми на основании гражданско-правовых договоров, при непосредственном участии администратора информационной безопасности.

63. Эксплуатация программного обеспечения состоит из следующих этапов:

а) определение потребности в программном обеспечении;

б) приобретение программного обеспечения;

в) установка (внедрение) программного обеспечения;

г) поддержка и сопровождение программного обеспечения;

д) удаление (вывод из эксплуатации) программного обеспечения.

64. В ходе определения потребности в программном обеспечении руководителем Учреждения, в котором планируется эксплуатация данного программного обеспечения, принимается решение о заявке на установку программного обеспечения:

а) при необходимости организации нового рабочего места, оснащенного средствами вычислительной техники;

б) при необходимости выполнения сотрудниками новых (дополнительных) обязанностей, для которых требуются дополнительное программное обеспечение или полная замена технических средств информационной системы;

в) при появлении качественно нового (альтернативного) программного обеспечения взамен уже используемых в составе информационных систем (при необходимости).

65. При наличии в Учреждении запрошенного программного обеспечения администратор информационной безопасности выполняет работы по его установке, за средством вычислительной техники закрепляются лицензии на установленное на нем программное обеспечение.

При отсутствии в Учреждении запрошенного программного обеспечения или вакантных лицензий на коммерческое программное обеспечение (из перечня в реестре разрешенного к использованию программного обеспечения), руководитель Учреждения инициирует заявку на приобретение программного обеспечения.

66. При установке (внедрении) программного обеспечения администратор информационной безопасности:

а) обеспечивает оперативный учет лицензий вводящегося в эксплуатацию программного обеспечения, организует работы по установке программного обеспечения на средства вычислительной техники;

б) готовит два экземпляра паспорта средства вычислительной техники или вносит изменения в имеющийся паспорт средства вычислительной техники. Один экземпляр паспорта средства вычислительной техники остается у сотрудника Учреждения, являющегося оператором средства вычислительной техники, другой хранится в архиве документов администратора информационной безопасности.

67. Любое изменение перечня установленного программного обеспечения отражается в паспорте средства вычислительной техники.

68. После установки программного обеспечения установочные комплекты (дистрибутивы) передаются администратору информационной безопасности.

69. Должностные лица, ответственные за эксплуатацию информационной системы, должны обеспечивать сохранность переданных им носителей с ключевой информацией, лицензионным программным обеспечением, сертификатов подлинности программного обеспечения.

70. Поддержка и сопровождение программного обеспечения выполняется администратором информационной безопасности, а при необходимости – техническими специалистами других организаций, привлекаемыми на основании гражданско-правовых договоров.

71. Осуществление поддержки и сопровождения программного обеспечения предусматривает, в том числе, выполнение следующих видов работ:

а) настройка установленного программного обеспечения;

б) установка обновлений программного обеспечения;

в) регламентированное создание резервных копий (архивирование) программного обеспечения и пользовательских данных (электронных документов, баз данных);

г) устранение неисправностей, связанных с использованием установленного программного обеспечения;

д) консультирование пользователей информационных систем.

72. Удаление (вывод из эксплуатации) программного обеспечения проводится в случаях:

а) окончания лицензионного срока использования программного обеспечения;

б) замены используемого программного обеспечения на альтернативное программное обеспечение или программное обеспечение более поздних версий;

в) прекращения использования программного обеспечения вследствие отсутствия необходимости, морального старения.

73. Вывод из эксплуатации выполняется администратором информационной безопасности, а при необходимости техническими специалистами других организаций, привлекаемыми на основании гражданско-правовых договоров.

74. При удалении (выводе из эксплуатации) программного обеспечения производится:

а) аудит программного обеспечения (далее – аудит) Учреждения;

б) удаление выводимого из эксплуатации программного обеспечения со всех средств вычислительной техники информационных систем;

в) при необходимости подготовка и передача специалисту Учреждения, осуществляющему бухгалтерский учет, акта вывода из эксплуатации программного обеспечения;

г) соответствующие отметки в паспортах средств вычислительной техники.

75. При необходимости администратор информационной безопасности организует хранение выведенного из эксплуатации программного обеспечения.

76. Аудит проводится в целях выявления несоответствия перечней фактически установленного программного обеспечения на средствах вычислительной техники перечням, зафиксированным в паспортах средств вычислительной техники. Аудит проводит администратор информационной безопасности.

77. При выявлении несоответствия перечня установленного программного обеспечения текущей версии паспорта средства вычислительной техники программное обеспечение, наименование которого отсутствует в паспорте средства вычислительной техники, подлежит немедленному удалению. Администратор информационной безопасности в этом случае вправе инициировать проведение служебной проверки для установления обстоятельств установки программного обеспечения, не предусмотренного паспортом средства вычислительной техники, а также выявления лиц, осуществивших эти действия.

78. Аудит проводится по мере необходимости, но не реже одного раза в 6 месяцев. Необходимость, время и область проведения аудита определяются в соответствии с настоящей Политикой руководителем учреждения.

Раздел XI
Использование беспроводных сетей в информационных системах Учреждения

79. В Учреждении разрешено использование «гостевых» беспроводных сетей, физически не пересекающихся с единой информационно-коммуникационной сетью Правительства Тверской области и локально-вычислительными сетями Министерства.

80. Запрещается подключение беспроводных сетей, а также доступ к единой информационно-коммуникационной сети Правительства Тверской области и локально-вычислительным сетям Министерства с различных устройств с использованием беспроводных сетей.

Раздел XII
Использование мобильных устройств и носителей информации в информационных системах Учреждения

81. Под использованием мобильных устройств и носителей информации в информационных системах понимается их подключение к информационным системам для приема, обработки, передачи информации

между информационными системами и мобильными устройствами, носителями информации.

82. В информационных системах допускается использование только учтенных мобильных устройств и носителей информации, которые являются государственной собственностью Тверской области и подвергаются регулярной ревизии (контролю).

83. На учтенных мобильных устройствах и носителях информации допускается использование коммерческого программного обеспечения, входящего в реестр разрешенного к использованию программного обеспечения.

84. Установка программного обеспечения на мобильные устройства осуществляется администратором информационной безопасности и/или сотрудником по информационной безопасности.

85. Установка на мобильные устройства программного обеспечения допускается только с интернет-ресурсов, рекомендуемых производителем мобильных устройств.

86. К учтенным мобильным техническим средствам информационных систем предъявляются те же требования по обеспечению информационной безопасности, что и к стационарным.

Целесообразность дополнительных мер обеспечения информационной безопасности определяется администратором информационной безопасности.

87. С учтенных мобильных технических средств информационных систем при необходимости разрешается доступ к электронной почте Министерства.

88. Запрещается подключение мобильных устройств к информационным системам, на которых обрабатывается информация ограниченного доступа, а также хранение информации ограниченного доступа на мобильных устройствах.

Раздел XIII
Порядок регистрации должностных лиц в межведомственных системах Учреждения

89. К межведомственным информационным системам Учреждения относятся системы электронного документооборота, системы корпоративной электронной почты, реестр государственных служащих Тверской области, иные территориально распределенные межведомственные информационные системы Министерства (далее – межведомственные информационные системы).

90. Руководитель Учреждения направляет в областной исполнительный орган государственной власти Тверской области,

уполномоченный на подключение к межведомственной информационной системе, заявку на регистрацию в межведомственной информационной системе должностных лиц, которая должна содержать:

а) наименование межведомственной информационной системы, в которой регистрируются должностные лица Учреждения;

б) должности, фамилии, имена и отчества должностных лиц, регистрируемых в межведомственной информационной системе.

Заявка также может содержать другую определяемую областным исполнительным органом государственной власти Тверской области, уполномоченным на подключение к межведомственной информационной системе информацию, включаемую в идентификационные данные.

91. После получения от Учреждения заявки на регистрацию должностных лиц в межведомственной информационной системе, ответственное должностное лицо областного исполнительного органа государственной власти Тверской области, уполномоченного на подключение к межведомственной информационной системе, регистрирует пользователей и проводит необходимые настройки.

92. Ответственное должностное лицо областного исполнительного органа государственной власти Тверской области, уполномоченного на подключение к межведомственной информационной системе, направляет необходимую ключевую информацию (ключевые файлы) администратору информационной безопасности Учреждения.

93. При увольнении должностного лица, зарегистрированного в межведомственной информационной системе, руководитель Учреждения в трехдневный срок со дня увольнения направляет в областной исполнительный орган государственной власти Тверской области, уполномоченный на подключение к межведомственной информационной системе, заявку об исключении уволенного сотрудника из пользователей межведомственной информационной системы.

Раздел XIV
Порядок использования средств криптографической защиты информации в Учреждении

94. Работы по приобретению средств криптографической защиты информации проводятся Учреждением по согласованию с уполномоченным областным исполнительным органом государственной власти Тверской области в сфере защиты информации.

95. Для работы с СКЗИ привлекаются уполномоченные должностные лица, назначенные соответствующим приказом Учреждения, которые получают и используют сертификаты ключей проверки электронной подписи

и ключи электронной подписи (далее – ключевая информация) и несут персональную ответственность за:

а) сохранение в тайне сведений конфиденциального характера, ставших им известными в процессе работы с СКЗИ;

б) сохранение в тайне содержания ключевой информации;

в) сохранность носителей ключевой информации и других документов о ключах, выдаваемых с ключевыми носителями.

96. В Учреждении должны быть обеспечены условия хранения носителей ключевой информации и карточки отзыва ключей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации и паролей отзыва ключей.

97. На средствах вычислительной техники информационных систем, на которых установлены средства шифрования и электронной подписи, не должно быть установлено и эксплуатироваться программное обеспечение, которое может нарушить функционирование программных СКЗИ. При обнаружении на рабочем месте, оборудованном СКЗИ, программного обеспечения, нарушающего работу указанных средств, работа с СКЗИ на данном рабочем месте должна быть прекращена и должны быть организованы мероприятия по анализу и ликвидации негативных последствий инцидента информационной безопасности.

98. При работе с СКЗИ не допускается:

а) разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер;

б) вставлять ключевой носитель в интерфейс технического средства информационной системы при проведении работ, не являющихся штатными процедурами использования ключей, а также в интерфейсы других технических средств информационной системы;

в) записывать на носителе ключевой информации постороннюю информацию;

г) вносить какие-либо изменения в программное обеспечение средств шифрования и электронной подписи;

д) использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования (при наличии возможности).

99. Посторонние лица не должны допускаться к работе со средствами вычислительной техники, на которых установлены средства шифрования и электронной подписи.

100. Уполномоченные должностные лица Учреждения, привлекаемые для работы с СКЗИ, отвечают за сохранность и конфиденциальность ключевой информации. В случае компрометации ключевой информации мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, переданной с использованием СКЗИ, организует руководитель руководитель, а осуществляют уполномоченные

должностные лица Министерства, привлекаемые для работы с СКЗИ, и администратор информационной безопасности.

101. При компрометации ключевой информации должностного лица Министерства данное должностное лицо должно немедленно прекратить действия, связанные с использованием данной ключевой информации, и поставить в известность представителя удостоверяющего центра о факте компрометации.

Раздел XV
Обеспечение физической защиты информационных систем Учреждения

102. Физическая защита информационных систем Учреждения обеспечивается комплексом мер по оборудованию зданий (помещений) средствами охранной сигнализации, организации постов охраны, опечатыванию помещений, организации и соблюдению внутриобъектового и пропускного режимов, порядка доступа в служебные помещения, хранению ключей от служебных помещений.

103. Физический доступ к информационным системам посторонних лиц не допускается.

104. Время прохода сотрудников в здание Учреждения устанавливается правилами внутреннего служебного распорядка.

105. Пропускной режим Учреждения устанавливается в соответствии с порядком, утвержденным Правительством Тверской области.

106. При отсутствии в помещениях сотрудников Учреждения двери в эти помещения должны быть закрыты на ключ. Вскрытие помещений при отсутствии лиц, имеющих на это право, осуществляется с разрешения руководителя Учреждения в случаях крайней необходимости.

107. В целях физической охраны серверов, информационных систем и баз данных, расположенных на выделенных технических средствах информационных систем, такие технические средства (при наличии возможности) размещаются в специально выделенных для этих целей помещениях. Доступ к таким техническим средствам ограничивается физически.

108. Двери помещений должны иметь достаточную степень защиты от возможного несанкционированного проникновения, быть исправными, хорошо подогнанными под максимально укрепленную дверную коробку.

Двери помещений и решетки на окнах (при их наличии) оснащаются замками и запирающими устройствами, обеспечивающими достаточную степень защиты от взлома. В качестве запирающих устройств, устанавливаемых на дверях и окнах, применяются врезные, накладные замки, задвижки, засовы, шпингалеты и т.п. Для запирания оконных решеток допускается применять висячие замки.

109. Окна, фрамуги и форточки (стеклопакеты) всех помещений закрываются на надежные и исправные запоры. Стекла надежно

закрепляются в пазах. Не допускается эксплуатация поврежденного остекления окон.

110. Ключи от замков на оконных решетках (при их наличии) и дверях запасных выходов располагаются в непосредственной близости от них, при этом принимаются меры, исключающие несанкционированный доступ к этим ключам посторонних лиц.

111. В Учреждении наряду с рабочими комплектами ключей при необходимости предусматриваются дополнительные комплекты ключей от всех помещений, распашных металлических решеток (при их наличии), основных и запасных выходов. Запасные комплекты ключей с соответствующими бирками хранятся в службе охраны здания, в котором размещается Учреждение.

112. Все экземпляры ключей учитываются в журнале регистрации ключей к замкам Учреждения. В указанный журнал вносится фамилия и должность сотрудников, от какого из помещений получены (сданы) ключи, с личной подписью сотрудника, получившего (сдавшего) экземпляр ключа. Наличие неучтенных ключей не допускается. В случае утраты рабочих или запасных экземпляров ключей об этом немедленно ставится в известность руководитель учреждения.

113. При необходимости опечатывания помещений сотрудникам выдаются номерные печати Учреждения (далее – номерные печати). Выдача номерных печатей оформляется приказом Учреждения и осуществляется под личную подпись в специальном журнале. Сотрудники, имеющие номерные печати, несут персональную ответственность за их сохранность. Проверки фактического наличия ключей от хранилищ и номерных печатей проводятся руководителем учреждения не реже одного раза в месяц.

114. Должностные лица Учреждения, осуществляющие сдачу помещений под охрану и их опечатывание, проверяют:

а) работоспособность средств охранной сигнализации (при ее наличии);

б) выключение освещения и потребителей электрической энергии (за исключением потребителей, питание которых необходимо непрерывно);

в) закрытие окон, решеток, форточек, закрытие и опечатывание дверей запасных выходов и размещение ключей от них в опечатанном виде рядом с дверями.

115. Ключи от помещений сдаются на пост охраны здания, в котором размещается оборудование.

116. При снятии помещений с охраны ответственные должностные лица:

а) после отключения сигнализации (при ее наличии) проверяют целостность печати на дверях и замках;

б) при обнаружении каких-либо повреждений замков, дверей, окон, форточек, фрамуг, не вскрывая их, вызывают представителей службы охраны и сообщают руководителю Учреждения для составления акта осмотра и проведения служебной проверки.

117. Для обеспечения электробезопасности информационных ресурсов Тверской области подключение информационных систем к электрической сети осуществляется в соответствии с государственными стандартами Российской Федерации, строительными нормами и правилами, а также правилами технической эксплуатации электроустановок потребителей, утвержденными приказом Министерства энергетики Российской Федерации от 13.01.2003 № 6 «Об утверждении Правил технической эксплуатации электроустановок потребителей».

118. Электропитание подводится к оборудованию от центрального электрического щита через автоматические выключатели. В качестве дополнительной защиты информационных ресурсов используются устройства защитного отключения. Все автоматические выключатели и устройства защитного отключения монтируются в соответствии с нагрузкой, потребляемой оборудованием.

Силовые и телекоммуникационные кабели защищаются от возможного несанкционированного подключения или повреждения.

119. Все технические средства информационных систем подключаются к электропитанию через источники бесперебойного питания, обеспечивающие корректное выключение или продолжительную работу.

Раздел XVI
Обслуживание технических средств информационных систем Учреждения

120. Еженедельное обслуживание технических средств информационных систем выполняется пользователем в соответствии с инструкцией по еженедельному техническому обслуживанию информационной системы (приложение 6 к Политике).

121. Другие виды работ по техническому обслуживанию информационной системы выполняются администратором информационной безопасности, а при необходимости – техническими специалистами других организаций, привлекаемыми на основании гражданско-правовых договоров.

122. Ремонтные работы на технических средствах информационных систем осуществляются только администратором информационной безопасности или техническими специалистами других организаций, привлекаемыми на основании гражданско-правовых договоров.

123. О факте выполнения работ по техническому обслуживанию информационных систем администратор информационной делает соответствующую отметку в журнале учета нештатных ситуаций, выполнения профилактических и ремонтных работ, установки и модификации технических средств и программного обеспечения по форме согласно приложению 7 к Политике.

Раздел XVII

Управление инцидентами информационной безопасности в Учреждении

124. Инциденты информационной безопасности подразделяются на:

а) внутренний инцидент – инцидент, источником которого является нарушитель, состоящий в служебных, трудовых и иных договорных отношениях с Учреждением (далее – внутренний нарушитель). К наиболее распространенным внутренним инцидентам информационной безопасности относятся:

утечка сведений конфиденциального характера;

неправомерный доступ к информации;

удаление информации;

компрометация информации;

саботаж;

мошенничество в информационных системах, с участием внутреннего нарушителя;

аномальная сетевая активность;

аномальное поведение программного обеспечения;

использование средств вычислительной техники Учреждения в личных целях или в мошеннических операциях;

б) внешний инцидент – инцидент, источником которого является нарушитель, не состоящий в служебных, трудовых и иных договорных отношениях с Учреждением (далее – внешний нарушитель). К наиболее распространенным внешним инцидентам относятся:

мошенничество в информационных системах с участием внешнего нарушителя;

атаки типа «отказ в обслуживании» (DoS), в том числе распределенные (DDoS);

перехват и подмена трафика;

размещение конфиденциальной/провокационной информации в ИТКС Интернет, касающейся Учреждения;

взлом, попытка взлома, сканирование сайтов Учреждения;

сканирование сети, попытка взлома сетевых узлов;

вирусные атаки;

неправомерный доступ к конфиденциальной информации;

анонимные письма (письма с угрозами).

125. Источником информации об инциденте информационной безопасности могут служить:

а) сообщения пользователей информационных систем;

б) уведомления компетентных органов;

в) данные, полученные на основании анализа электронных журналов регистрации информационных систем, систем защиты.

126. При получении сообщения об инциденте информационной безопасности по электронной почте или по телефонному звонку необходимо убедиться в достоверности полученной информации (например, путем

совершения «обратного» звонка по указанным в сообщении телефонам, проверки данных, указанных в подписи сообщения или названных при звонке).

127. Сотрудник, получивший информацию об инциденте информационной безопасности, сообщает об этом администратору информационной безопасности и руководителю Учреждения.

Администратор информационной безопасности обязан принять меры по локализации инцидента информационной безопасности и минимизации потерь от инцидента информационной безопасности для Учреждения.

128. Администратор информационной безопасности регистрирует инцидент в журнале учета нештатных ситуаций, выполнения профилактических и ремонтных работ, установки и модификации технических средств и программного обеспечения.

129. Для анализа инцидентов информационной безопасности создается комиссия, в состав которой включаются:

а) руководитель Учреждения, ответственный за организацию защиты информации;

б) руководитель структурного подразделения Учреждения, в котором произошел инцидент;

в) администратор информационной безопасности.

130. Комиссия собирает и анализирует все данные об обстоятельствах инцидента информационной безопасности (электронные письма, журналы событий информационных систем, показания сотрудников и др.), устанавливает факт наличия (отсутствия) утечки информации ограниченного доступа и обстоятельства ей сопутствующие, определяет перечень лиц, виновных в нарушении предписанных мероприятий по защите информации, устанавливает причины и условия, способствовавшие нарушению.

131. По итогам работы комиссии ответственный за организацию защиты информации, готовит руководителю Учреждения заключение, в котором указываются причина возникновения инцидента, последствия инцидента, лица, виновные в возникновении инцидента, предложения о наказании виновных лиц и мерах по недопущению подобных инцидентов в будущем.

Раздел XVIII
Политика кадровой безопасности в Учреждении

132. Обучение сотрудников Учреждения, имеющих право доступа к информационной системе, правильному обращению с информацией (базами данных), содержащейся в информационной системе, осуществляется должностным лицом, ответственным за эксплуатацию информационной системы, а также администратором информационной безопасности.

133. Обучение вопросам защиты информации должно предусматривать необходимость сохранения конфиденциальности всей информации,

требующей обеспечения конфиденциальности, циркулирующей в информационной системе.

134. Все сотрудники Учреждения предупреждаются об условиях конфиденциальности информации о персональных данных субъектов персональных данных, содержащихся в информационных системах, способах и методах защиты информационных систем и недопустимости разглашения такой информации.

Раздел XIX
Политика безопасности при работе с третьими лицами в Учреждении

135. Все действия по техническому обслуживанию, ремонту, установке и замене технических средств информационных систем, прокладке кабеля, переустановке и обновлению программного обеспечения проводятся исключительно с разрешения Учреждения в присутствии администратора информационной безопасности.

136. Работы, указанные в пункте 147 настоящего раздела, регистрируются администратором информационной безопасности в журнале учета нештатных ситуаций, выполнения профилактических и ремонтных работ, установки и модификации технических средств и программного обеспечения.

137. При выполнении работ, указанных в пункте 147 настоящего раздела, администратор информационной безопасности не должен допускать установку поставщиками в информационных системах дополнительного программного обеспечения (бэкдоров) с целью защиты, изменения и обновления своих продуктов.

138. Отчуждаемые носители информации должны пройти полную очистку (безвозвратное стирание информации) с использованием общего или специального программного обеспечения.

Если произвести очистку информации невозможно, то носители информации должны быть физически уничтожены.

139. Перед передачей оборудования другим предприятиям и организациям необходимо удалить с него всю информацию, требующую обеспечения конфиденциальности.

140. Все работы, указанные в пункте 147 настоящего раздела, проводимые сторонними организациями, осуществляются только на основании гражданско-правовых договоров, в которых отдельным пунктом должно определяться обязательство о неразглашении полученной третьими лицами информации ограниченного доступа.

Приложение 1
К Политике информационной безопасности
ГБУ «ТверьИнформОбр»

Перечень информационных систем ГБУ «ТверьИнформОбр»

№ п/п	Наименование информацион-ной системы	Тип информацион-ной системы в зависимости от категории информации	Масштаб информационной системы (федеральный, региональный, объектовый)	Количество пользователей информацион-ной системы	Средства вычислительной техники информационной системы (кол-во)	Должностное лицо, ответственное за эксплуатацию информационной системы
3	Автоматизированная система управления сферой образования Тверской области (АСУ СО ТО)	ИСПДн	Региональный	960	960	И.о. заместителя директора ГБУ «ТверьИнформОбр» Строганов А.В.

И.о. директора
ГБУ ТверьИнформОбр»

М.В. Пищулин