«УТВЕРЖДАЮ»
Директор ГБУК «ТОДНТ»
_____ Е.Г. Марина
"_____" _____ 2021 г.

Положение о Политике информационной безопасности в государственном бюджетном учреждении культуры Тверской области «Тверской областной Дом народного творчества»

Раздел I
Общие положения

1.Настоящее Положение разработано в соответствии с действующим законодательством Российской Федерации, распоряжением Правительства Тверской области от 12.10.2017 г. № 345-рп «Об утверждении Политики информационной безопасности исполнительных органов государственной власти Тверской области и государственных унитарных предприятий Тверской области», нормативными актами и соотносимыми с ними положениями внутренних документов Тверского областного Дома народного творчества (далее – «ТОДНТ»). Положение представляет собой совокупность правил, процедур, практических приемов и общих принципов защиты информациис целью обеспечения информационной безопасности (далее - ИБ) в осуществлении текущей деятельности, перспективном развитии информационных систем.

2. Целями реализации Политики являются минимизация ущерба от реализации угроз безопасности информациив «ТОДНТ» при использовании информационных технологий.

3. В ходе реализации Политики организация руководствуется следующими принципами:

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

3.2 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;

3.3 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;

3.4 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;

3.5 принцип экономической целесообразности, в соответствии с которым при реализации мероприятий по обеспечению информационной безопасности, расходы бюджета организации на эти цели соизмеряются с вероятным ущербом от реализации угроз информационной безопасности;

3.6 принцип своевременности, подразумевающий упреждающий характер мероприятий по обеспечению информационной безопасности и осуществление модернизации средств защиты информации при внесении изменений в существующие информационные системы;

4. Для целей Политики применяются следующие термины:

4.1 специалист информационной безопасности – сотрудник учреждения (ведущий инженер-программист), ответственный за соблюдение требований законодательства в сфере защиты информации, назначенный приказом учреждения;

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

4.3 инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность организации (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);

4.4 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;

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

4.6 пользователь информационной системы (средства вычислительной техники) – сотрудник учреждения, участвующий в функционировании информационной системы (средства вычислительной техники) или использующий результаты ее функционирования;

4.7 программное обеспечение – совокупность программных средств и программных продуктов;

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

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

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

4.11 средство вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (коммутаторное оборудование, роутеры, средства хранения данных, компьютеры, средства хранения ключевой информации, программное обеспечение, кассовые аппараты);

4.12 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;

4.13 учетная запись «специалист» – 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);

4.14 сотрудник, ответственный за реализацию политики информационной безопасности и поддержание ее в актуальном состоянии, назначается приказом директора «ТОДНТ»;

4.15 рабочая станция – это компьютер, включенный в состав локальной сети учреждения, закрепленный за рабочим местом сотрудника с совокупностью подключенного периферийного оборудования (коммутатор, роутер, принтер, сканер, копировальное устройство, кассовый аппарат, средства хранения данных).

5. Предметом настоящего Положения является:

- порядок и управление доступом к информационным системам, персональным данным, конфиденциальной информации;
- рекомендации работы с почтовыми программами;
- защита информационных систем от несанкционированного доступа;
- управление и контроль доступа к удаленным рабочим местам;
- управление доступом к телекоммуникационному оборудованию (телефонная станция), кабельной инфраструктуре здания, коммутаторному оборудованию (коммутаторная);
- разграничение прав доступа на разделяемые информационные, программные и сетевые ресурсы;
- рекомендации по внедрению программ из Единого реестра российских программ для электронных вычислительных машин и баз данных;
- использование ресурсов глобальных информационных, справочных систем и порталов Интернет;
- защита рабочих станций и пользователей локальной сети от внешних и внутренних атак, информационных угроз, антивирусная защита;
- дублирование, резервирование и раздельное хранение конфиденциальной информации;
- обеспечение бесперебойного функционирования технических, программных и информационных систем, сайта организации.

Раздел II
Управление доступом к информационным системам и конфиденциальной информации организации

1. В целях обеспечения защиты информации в «ТОДНТ», устанавливается следующий порядок допуска к работе с конфиденциальными источниками:

- Решение о доступе работника к определенному виду конфеденциальной информации принимается Директором «ТОДНТ».
- Специалист информационных технологий обеспечивает управление доступом к файлам и сетевым ресурсам авторизованным лицам.
- Доступ к сегментам компьютерной сети «ТОДНТ»рекомендовано осуществлять с персональным паролем. Пользователь должен держать в тайне свой пароль. Сообщать свой пароль другим лицам, а также пользоваться чужими паролями запрещается. Имя пользователя и пароль на вход в информационные системы, почту или порталы должны быть

отличны от имени пользователя и пароля доступа в общую компьютерную сеть.

- Категорически запрещается снимать несанкционированные копии с носителей конфиденциальной или персональной информации, знакомить с содержанием электронной информации лиц, не допущенных к этому.

2. Для защиты он несанкционированного доступа к конфиденциальной информации средствам вычислительной техники применяется разграничение физического доступа пользователей.

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

3.1 для управления доступом к информационным системам в «ТОДНТ» существует разрешительная система допуска пользователей к рабочим станциям, информационным системам и связанным с их использованием работам и документам;

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

3.3 при любом оставлении сотрудником рабочего места средство вычислительной техники информационной системы рекомендовано блокировать и требовать аутентификации для дальнейшего продолжения работы;

3.4 каждому сотруднику «ТОДНТ», имеющему право доступа к информационным системам, присваивается отличная от других учетная запись пользователя с правами доступа к определенным сетевым ресурсам;

3.5 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, передавать вверенный ему пароль или иные средства аутентификации другим сотрудникам в случае служебной необходимости с ведома директора «ТОДНТ».

4. 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.

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

6. О выявленных попытках несанкционированного доступа к информационным системам специалист информационной безопасности незамедлительно сообщает директору «ТОДНТ» служебной запиской.

Раздел III
Основные правила и методы предотвращения неавторизованного доступак информациис использованием парольной аутентификации

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

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

3. Пароли специалиста информационной безопасности подлежат хранению в сейфе, закрепленным за специалистом информационной безопасности, в запечатанном конверте с указанием наименования информационной системы, должности, фамилии, инициалов должностного лица, ответственного за эксплуатацию информационной системы.

4. Порядок хранения и использования паролей определяет специалист информационной безопасности.

5. Пароль пользователя информационной системы должен отвечать следующим требованиям:

5.1 длина пароля должна быть не менее 8 символов;

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

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

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

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

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

5.7 пароль должен быть уникальным по отношению к паролям других учетных записей данного пользователя;

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

7. При компрометации пароля пользователь должен сообщить об этом специалисту информационной безопасности и незамедлительно сменить пароль.

8. При удаленном доступе к рабочим станциям по обслуживанию бухгалтерских и кассовых программ, доступ осуществляется техническими специалистами других организаций, привлекаемыми на основании гражданско-правовых договорови при визуальном контроле сотрудников «ТОДНТ», ответственных за рабочее место.

Раздел IV
Основные правила и методы организации антивирусной защиты информационных систем учреждения

1. Организация антивирусной защиты в «ТОДНТ», а также контроль за выполнением мероприятий по антивирусной защите возлагаются на специалиста информационной безопасности.

2. На специалиста информационной безопасности возлагаются следующие функции:

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

2.2 организация и проведение технических мероприятий по антивирусной защите;

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

3. 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.

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

5. Для антивирусной защиты информационных систем «ТОДНТ» рекомендовано использовать (заменять ранее использующиеся) официально приобретенные средства антивирусной защиты, сведения о которых содержатся в Государственном реестре сертифицированных средств защиты информации или в Едином реестре российских программ для электронных вычислительных машин и баз данных.

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

7. Для периодических проверок объектов антивирусной защиты использовать средства антивирусной защиты различных производителей.

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

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

10. 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 со специалистом информационной безопасности проводят внеочередной антивирусный контроль средства вычислительной техники.

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

11.1 приостановить работу;

11.2 немедленно поставить в известность об этом специалиста информационной безопасности, владельца зараженных файлов (ресурсов), а также других сотрудников, использующих эти файлы в работе;

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

11.4 провести лечение или уничтожение зараженных файлов.

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

13. 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 V
Основные правила и методы организации резервного копирования

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

2. Специалист информационной безопасности в зависимости от функциональных особенностей эксплуатируемых информационных систем определяет перечень данных, подлежащих резервному копированию и хранению, расписание резервного копирования.

3. Резервному копированию подлежит информация следующих основных категорий:

- рабочая станция директора «ТОДНТ», рабочие станции бухгалтеров и базы данных 1С;
- групповая информация пользователей (общие каталоги подразделений);
- информация, необходимая для восстановления рабочих станций и баз данных;
- рабочие копии установочных компонент программного обеспечения вычислительных средств информационных систем;
- рабочие материалы, фильмы, фотографии, сценарии, отчеты, которые представляют архив работы «ТОДНТ».

4. Для ведения архивов выделяются переносные, съемные носители информации, дополнительные жесткие диски на рабочих станциях.

5. Проводится архивирование записей мероприятий на CD и DVD носителях в подарочном формате.

6. Выкладываются фильмы на канале youtube.com «ТОДНТ».

7. Предоставляются копии фильмов мероприятий по запросу граждан, с разрешения директора «ТОДНТ».

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

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

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

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

8. О выявленных попытках несанкционированного доступа к резервируемой информации конфиденциального характера, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, специалист информационной безопасности сообщает директору «ТОДНТ» служебной запиской в течение рабочего дня после обнаружения указанного события.

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

Раздел VI
Порядок работы с электронной почтой в «ТОДНТ»

1. Электронная почта в «ТОДНТ» должна использоваться только в служебных целях.

2. При работе с электронной почтой сотрудникам «ТОДНТ»**запрещается**:

2.1 использовать адрес служебной электронный почты в личных целях;

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

2.3 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;

2.4 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;

2.5 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.;

2.6 распространять или получать посредством сообщений электронной почты информацию, содержащую персональные данные,служебные сведения ограниченного доступа, сведения, относящиеся к государственной тайне. Если такая пересылка обусловлена производственной необходимостью, то посылаются архивы файлов, защищенные паролем. Письма с такими архивными файлами из почты полностью удаляются после их обработки.

Раздел VII
Порядок использования информационно-телекоммуникационной сети Интернет

1. Доступ к информационно-телекоммуникационную сеть Интернет (ИТКС Интернет) в «ТОДНТ» может предоставляться сотрудникам в целях выполнения ими своих служебных обязанностей.

2. Подключение средств вычислительной техники к ИТКС Интернет выполняется специалистом информационной безопасности.

3. При использовании ИТКС Интернет сотруднику организации**запрещено**:

3.1 использовать предоставленный доступ к ИТКС Интернет в личных целях;

3.2 использовать специализированные аппаратные и программные средства, позволяющие сотрудникам получить несанкционированный доступ к ИТКС Интернет. Если это обусловлено производственной необходимостью подготовки и проведения мероприятий, то установка и использование производится с разрешения директора «ТОДНТ»;

3.3 совершать действия, направленные на нарушение функционирования элементов информационных систем;

3.4 публиковать, загружать и распространять материалы, содержащие:

- информацию ограниченного доступа;
- публиковать фото, видео детей и подростков без предварительного согласия их родителей;
- 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.

4. При необходимости,специалист информационной безопасности имеет право блокировать доступ к интернет-ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей с разрешения директора «ТОДНТ».

5. При проведении мероприятий в «ТОДНТ» и выездных мероприятий в области с участием детей и подростков, родители участников заполняют форму «Согласие на фото, видеосъемку, обнародование изображений, передачу в эфир». Сведения носят конфиденциальный характер и хранятся в соответствии правил хранения конфиденциальной информации и персональных данных.

Раздел VIII
Использование программного обеспечения в информационных системах

1. В «ТОДНТ», для выполнения возложенных на него функций, разрешено применение ограниченного перечня коммерческого и свободного программного обеспечения.

2. Перечень программного обеспечения, разрешенного к использованию определяется специалистом информационной безопасности.

3. Перечень программного обеспечения, устанавливаемого на средство вычислительной техники, определяется специалистом информационной, исходя из должностных обязанностей пользователя, а также функций информационной системы и заносится специалистом информационной безопасности в паспорт рабочего места.

4. Самостоятельная установка и использование сотрудником организации программного обеспечения запрещается.

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

6. Эксплуатация программного обеспечения состоит из следующих этапов:

- определение потребности в программном обеспечении;
- приобретение программного обеспечения;
- установка (внедрение) программного обеспечения;
- поддержка и сопровождение программного обеспечения;
- удаление (вывод из эксплуатации) программного обеспечения.

7. Определение потребности в новом или дополнительном программном обеспечении согласовывается с директором«ТОДНТ»:

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

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

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

8. При наличии в «ТОДНТ» запрошенного программного обеспечения специалист информационной безопасности выполняет работы по его установке, за средством вычислительной техники закрепляются лицензии на установленное на нем программное обеспечение.

При отсутствии в «ТОДНТ» запрошенного программного обеспечения или вакантных лицензий на коммерческое программное обеспечение (из перечня в реестре разрешенного к использованию программного обеспечения), директор «ТОДНТ» инициирует заявку на приобретение программного обеспечения.

9. При установке (внедрении) программного обеспечения специалист информационной безопасности:

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

9.2 готовит паспорт средства вычислительной техники или вносит изменения в имеющийся паспорт средства вычислительной техники;

9.3 любое изменение перечня установленного программного обеспечения отражается в паспорте средства вычислительной техники.

10. После установки программного обеспечения установочные комплекты (дистрибутивы) передаются специалисту информационной.

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

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

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

- настройка установленного программного обеспечения;
- установка обновлений программного обеспечения;
- регламентированное создание резервных копий (архивирование) программного обеспечения и пользовательских данных (электронных документов, баз данных);
- устранение неисправностей, связанных с использованием установленного программного обеспечения;
- консультирование пользователей программных и информационных систем.

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

- окончания лицензионного срока использования программного обеспечения;
- замены используемого программного обеспечения на альтернативное программное обеспечение или программное обеспечение более поздних версий;
- прекращения использования программного обеспечения вследствие отсутствия необходимости, морального старения.

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

16. При необходимости специалист информационной безопасности организует хранение выведенного из эксплуатации программного обеспечения.

17. 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.

Специалист информационной безопасности в этом случае вправе инициировать проведение служебной проверки для установления обстоятельств установки программного обеспечения, не предусмотренногопаспортом средства вычислительной техники, а также выявления лиц, осуществивших эти действия.

Раздел IX
Использование беспроводных сетей в информационных системах

1. В «ТОДНТ» разрешено использование беспроводной сети по производственной необходимости во время проведения мероприятий при согласовании с директором «ТОДНТ».

2. Необходимость наличия беспроводной сети указывается в техническом задании к мероприятию.

3. Запрещается подключение к беспроводной сети в личных целях, так как это значительно уменьшает работоспособность сети на станциях всей организации.

Раздел X
Использование мобильных устройств и носителей информации

1. 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.

2. В информационных системах допускается использование мобильных устройств и учтенных носителей информации.

3. На учтенных носителях информации допускается использование коммерческого программного обеспечения, входящего в реестр разрешенного к использованию программного обеспечения.

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

5. С мобильных технических средств информационных систем, при необходимости, разрешается доступ к электронной почте организации.

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

7. При выходе из строя учтенного носителя информации, работы по восстановлению данных проводятся специалистом информационной безопасности.

Раздел XI
Порядок использования средств криптографической защиты информации

1. Для работы с СКЗИ привлекаются уполномоченные должностные лица, назначенные соответствующим приказом «ТОДНТ», которые получают и используют сертификаты ключей проверки электронной подписи и ключи электронной подписи (далее – ключевая информация) и несут персональную ответственность за:

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

1.2 сохранение в тайне содержания ключевой информации;

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

2. В «ТОДНТ», участвующем в информационном обмене электронными документами по телекоммуникационным каналам связи, должны быть обеспечены условия хранения носителейключевой информации и карточки отзыва ключей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации и паролей отзыва ключей.

3. 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.

4. При работе с СКЗИ не допускается:

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

4.2 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;

4.3 записывать на носители ключевой информации постороннюю информацию;

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

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

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

6. Уполномоченные должностные лица «ТОДНТ», привлекаемые для работы с СКЗИ, отвечают за сохранность и конфиденциальностьключевой информации.

7. Носители ключевой информации, пароли и прочая конфиденциальная информация хранится в сейфе ответственного уполномоченного должностного лица.

8. Доступ в помещение посторонним лицам запрещен. Технический персонал, осуществляющий уборку помещения, ремонт оборудования, может находиться в помещении только в присутствии работников, имеющих право находиться в помещении в связи с выполнением своих должностных обязанностей.

Раздел XII
Управление сетевой безопасностью при использовании сетевых ресурсов

1. Пользователям информационно-телекоммуникационной сети «ТОДНТ» **запрещается**:

- осуществлять попытки несанкционированного проникновения в чужие информационные системы;
- производить попытки присвоения себе чужих сетевых атрибутов (в частности сетевых адресов, MAC-адресов сетевых карт);
- предоставлять ресурсы своих технических средств посторонним пользователям для несанкционированного использования государственных информационных ресурсов Тверской области;
- размещать в информационных системах коммерческие и лицензионные программные средства, мультимедийные и информационные материалы с нарушением соответствующих авторских прав;
- распространять через информационно-телекоммуникационную сеть заведомо оскорбляющую честь и унижающую достоинство граждан информацию, материалы рекламного и коммерческого характера;
- использовать внешний мультимедийный трафик типа интернет-видео, музыкальных сетевых радиостанций, а также трафик пиринговых сетей, если это не связано с исполнением служебных обязанностей. При

возникновении трафика данного типа соответствующие сетевые коммуникации должны блокироваться специалистом информационной безопасности без предупреждения пользователя.

2. На технических средствах информационных систем, используемых для работы в информационно-телекоммуникационной сети рекомендуется устанавливать необходимые обновления программного обеспечения.

3. При существенном падении скорости передачи данных в информационно-телекоммуникационной сети, специалист информационной безопасности организует временную блокировку проблемного трафика до устранения самого проблемного трафика и вызвавших его причин.

4. Специалист информационной безопасности по согласованию с директором «ТОДНТ» с целью защиты сетевой инфраструктуры и пользователей, может блокировать спам и вирусные рассылки (как входящие, так и исходящие) вплоть до временного прекращения всех коммуникаций с хостами, вовлеченными в эти инциденты информационной безопасности (спамовые рассылки, вирусные и хакерские атаки), даже если это повлечет за собой временную невозможность доступа пользователей к легальным ресурсам этих хостов.

5. Особо крупные сетевые скачивания (дистрибутивы, ISO-образы дисков и т.п.) рекомендуется производить только с доверенных серверов и в нерабочее время, когда загрузка канала существенно меньше.

Раздел XIII
Обеспечение безопасности информации при проведении телефонных переговоров и видеоконференцсвязей

1. В целях обеспечения конфиденциальности телефонных переговоров в «ТОДНТ», не рекомендуется передавать по телефону информацию, содержащую служебные сведения ограниченного доступа, персональные данные, данные о времени и местонахождении членов Правительства Тверской области, руководителей ИОГВ Тверской области, государственных учреждений, унитарных предприятий Тверской области, если это не обусловлено служебной необходимостью.

2. В случае необходимости проведения конфиденциальных переговоров, такие переговоры проводятся в специально предназначенных для этого помещениях (кабинет директора).

3. Использовать для проведения видеоконференцсвязей разрешенные программы, рекомендованные вышестоящими организациями.

Раздел XIV
Обеспечение физической защиты информационных систем

1. Физическая защита информационных систем «ТОДНТ»обеспечивается комплексом мер по оборудованию зданий (помещений) средствами охранной сигнализации, видеонаблюдения, организации постов охраны, порядка доступа в служебные помещения, хранению ключей от служебных помещений, защиты телекоммуникационного оборудования.

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

3. Время прохода сотрудников в здания «ТОДНТ» устанавливаются правилами внутреннего служебного распорядка и приказами на работу сотрудников в выходные и праздничные дни.

4. При отсутствии в помещениях сотрудников «ТОДНТ» двери в эти помещения должны быть закрыты на ключ. Вскрытие помещений при отсутствии лиц, имеющих на это право, осуществляется с разрешения директора «ТОДНТ» в случаях крайней необходимости.

5. В целях физической охраны рабочих станций, 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.

6. Управление доступом к телекоммуникационному оборудованию (телефонной станции), коммутаторному оборудованию (коммутаторной) регулируется нормативными документами «ТОДНТ», оборудование защищено специальным шкафом.

7. 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.

8. Окна, фрамуги и форточки (стеклопакеты) всех помещений закрываются на надежные и исправные запоры. Стекла надежно закрепляются в пазах. Не допускается эксплуатация поврежденного остекления окон.

9. 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.

10. В «ТОДНТ» наряду с рабочими комплектами ключей при необходимости предусматриваются дополнительные комплекты ключей от всех помещений, распашных металлических решеток (при их наличии), основных и запасных выходов.

11. Все экземпляры ключей от служебных помещений учитываются в журнале регистрации ключей к замкам помещений «ТОДНТ». 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 директора «ТОДНТ».

12. Сотрудники «ТОДНТ», осуществляющие сдачу помещений под охрану, **проверяют:**

- выключение освещения и потребителей электрической энергии (за исключением потребителей, питание которых необходимо непрерывно);
- закрытие окон, решеток, форточек, закрытие и опечатывание дверей запасных выходов и размещение ключей от них в опечатанном виде рядом с дверями;
- выключение рабочих станций, кроме станции главного бухгалтера для обеспечения работы касс организации в выходные дни.

13. Ключи от помещений сдаются на пост охраны зданий.

14. 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».

15. 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.

16. Рекомендуется технические средства информационных систем подключать к электропитанию через источники бесперебойного питания, обеспечивающие корректное выключение или продолжительную работу.

Раздел XV
Обслуживание технических средств информационных систем

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

2. Профилактические и ремонтные работы на технических средствах информационных систем осуществляются только специалистом информационной безопасности или техническими специалистами других организаций, привлекаемыми на основании гражданско-правовых договоров.

3. О факте выполнения работ по техническому обслуживанию информационных систем специалист информационной безопасности делает соответствующую отметку в журнале учета нештатных ситуаций, выполнения профилактических и ремонтных работ, установки и модификации технических средств и программного обеспечения.

4. Рекомендации по еженедельному техническому обслуживанию рабочих станций:

4.1 Еженедельное техническое обслуживание технических средств рабочих станций проводится пользователем не реже 1 раза в неделю в один и тот же день недели.

4.2 В ходе еженедельного технического обслуживания выполняются следующие виды работ:

а) осмотр состояния кабелей, розеток, разъемов;

б) удаление загрязнений с внешних поверхностей блоков:

- клавиатуры;
- монитора;
- принтера;
- сканера;
- других устройств;

в) диагностика технических средств информационной системы, в ходе которой проводятся:

- проверка рабочих станций на наличие вирусов с помощью средств антивирусной защиты;
- резервное копирование данных;

- очистка диска от временных и неиспользуемых файловс помощью встроенных средств или специального программного обеспечения;
- проверка дисков и внешних накопителей на наличие ошибок;
- проверка работоспособности клавиш клавиатуры;
- проверка работоспособности сетевого подключения.

4.3 Для удаления загрязнений в виде пыли с пластмассовых и металлических поверхностей технических средств используется ткань или специальные салфетки. С поверхности монитора жирные пятна удаляются специальными салфетками. Въевшиеся отложения с пластмассовых поверхностей удаляются мыльным раствором (при очистке клавиш необходимо исключить попадание водного раствора вовнутрь клавиатуры и манипулятора). Запрещается использовать для очистки мониторов с антибликовыми покрытиями любые растворы.

4.4 Перед удалением загрязнений с технических средств рабочих станций их необходимо выключить.

4.5 При обнаружении повреждений электрических розеток, кабелей, в том числе заземления, необходимо срочно вызвать электрика.

5. При проведении технического обслуживания **запрещается**:

- использовать для очистки жесткие предметы (авторучки, карандаши, ножи, линейки и др.);
- подключать и отключать технические средства при включенном электропитании;
- снимать (открывать) крышки системных блоков.

6. При выявлении неисправностей технических средств рабочей станции, или программного обеспечения пользователь должен немедленно обратиться к специалисту информационной безопасности или техническому специалисту других организаций, привлекаемых на основании гражданско-правовых договоров.

Приложение 1

ПАСПОРТ
рабочего места

по состоянию на «_____» _____ 2021 года

_____

(кабинет, наименование подразделения)

Материально-техническое и программное обеспечение

	Инвентарный №	Характеристики, марка, габариты	Особенности	Установка, ремонт, перемещения	Примечание, рекомендации
Имя станции					
Системный блок, ОЗУ					
Монитор					
Клавиатура					
Мышь					
Колонки					
Принтер, кассовый ап.					
Сканер, Копир					
Коммутатор, модем, оборуд.					

Программное обеспечение

	Название, версия, назначение	Установка	Лицензия	Замечания, рекомендации
Операц.система				
Офисные программы				
Антивирус				
Криптозащита				

	Название, установка	Лицензия	Название, установка	Лицензия
Рабочие, основные программы				

ФИО, подпись ответственного лица (лиц):

Дата

Приложение 2

Журнал учета нештатных ситуаций, выполнения профилактических и ремонтных работ, установки и модификации технических средств и программного обеспечения

_____

наименование государственного учреждения Тверской области

№ п/п	Дата	№ технического средства, имя рабочей станции, кабинет	Краткое описание выполненной работы, нештатной ситуации	Наименование организации, выполнявшей работы, Ф.И.О. исполнителей и их подписи	Ф.И.О., подпись ответственного пользователя технического средства	Ф.И.О., подпись администратора информационной безопасности	Примечание (реквизиты и краткое содержание заявки)
1	2	3	4	5	6	7	8