



ЦЕНТР
ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ

Курс по информационной безопасности



Что такое информация?

Согласно Федеральному закону №149 от 27.07.2006 «Об информации, информационных технологиях и о защите информации»:

- **Информация** – это сведения (сообщения, данные) независимо от формы их представления.
- Информация в зависимости от категории доступа к ней подразделяется на **общедоступную информацию**, а также на информацию, доступ к которой ограничен федеральными законами (**информация ограниченного доступа**).
- Обязательным является соблюдение **конфиденциальности информации**, доступ к которой ограничен федеральными законами.
- Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим **коммерческую тайну, служебную тайну** и иную тайну, обязательность соблюдения **конфиденциальности** такой информации, а также ответственность за ее разглашение.

Конфиденциальная информация

Согласно Указу Президента РФ №188 от 06.03.1997 «Об утверждении перечня сведений конфиденциального характера» к конфиденциальной информации относятся:

- **Сведения** о фактах, событиях и обстоятельствах частной жизни гражданина, **позволяющие идентифицировать его личность (персональные данные)**
- Сведения, составляющие **тайну следствия и судопроизводства**
- Служебные сведения, доступ к которым ограничен органами государственной власти (**служебная тайна**)
- Сведения, связанные с **профессиональной деятельностью** (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров и так далее)
- Сведения, связанные с коммерческой деятельностью (**коммерческая тайна**)
- **Сведения о сущности изобретения**, полезной модели или промышленного образца до официальной публикации информации о них
- Сведения, содержащиеся в **личных делах осужденных**, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц
- **Защищаемая информация** – это информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Персональные данные

Согласно Федеральному закону №152 от 27.07.2006 «О Персональных данных»:

Персональные данные (далее ПДн) - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (**субъекту персональных данных**)

Закон регулирует отношения связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, иными муниципальными, юридическими лицами и физическими лицами с использованием средств автоматизации или без использования таких средств.

- **обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая **сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных**
- **оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами **организующие и (или) осуществляющие обработку персональных данных**, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными
- **конфиденциальность персональных данных** - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом **требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания**

Обработка персональных данных

Согласно Постановлению Правительства РФ №687 от 15.09.2008 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»:

- **Предоставление персональных данных** – действия (операции) с персональными данными, направленные на раскрытие персональных данных **определенному лицу или определенному кругу лиц**
- **Распространение персональных данных** - действия, направленные на раскрытие персональных данных **неограниченному кругу лиц**, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом
- **Уничтожение персональных данных** - действия, в результате которых **невозможно восстановить содержание персональных данных** в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители ПДн

Приказы, утвержденные в Правительстве ТО

Во исполнении требований законодательства Российской Федерации и подзаконных актов по защите информации в Правительстве ТО были утверждены Приказы, связанные с защитой информации:

- №6-осн от 18.01.2019 «Об утверждении Инструкции пользователя региональной информационной системы правительства ТО»
- №88-осн от 19.08.2019 «Об утверждении Регламента по организации парольной защиты в региональных информационных системах ТО»
- №83-осн от 30.10.2017 «Об утверждении Инструкции по применению машинных носителей информации в ОИВ ТО, АП ТО и ПУ»
- №90-осн от 20.07.2016 «Об использовании мобильных устройств и беспроводных точек доступа в региональной сети передачи данных АП ТО и ОИВ ТО»
- №57-осн от 07.05.2018 «Об утверждении Инструкции по порядку использования и организации работы со средствами криптографической защиты информации в РИС ТО»
- №101-осн от 20.08.2021 «Об утверждении перечня и порядка использования программного обеспечения в АП ТО, ОИВ ТО и ПУ»
- №132-осн от 26.10.2021 «Об утверждении регламентов безопасности мобильных устройств»
- №42-осн от 09.04.2019 «Об утверждении регламента защиты информации от несанкционированного доступа в РИС ТО»
- №109-осн от 27.08.2021 «Об утверждении политики антивирусной защиты информации в ОИВ ТО, АП ТО, ПУ»

Инструкция пользователя РИС ПТО

Пользователь **обязан**:

- Соблюдать **конфиденциальность** информации, обрабатываемой с использованием РИС ПТО (Региональная Информационная Система Правительства Тульской области)
- Покидая рабочее место, **блокировать** компьютер с помощью комбинации клавиш **Win+L**
- Сообщать в службу поддержки (т. 24-83-83) или администратору безопасности о **неработоспособности** средств защиты информации и в случае возникновения сообщения об **ошибке** в работе программного обеспечения и средств защиты информации
- При получении на рабочую электронную почту **подозрительных писем**, поступивших с незнакомого адреса, содержащих ссылки на скачивание файлов или вложение, переслать его как вложение на почтовый ящик servicedesk@tularegion.ru и spam@tularegion.ru с пометкой «*Прошу проверить на спам*». Переходить по ссылкам и скачивать вложения можно только **после** получения сообщения от специалиста о том, что вирусов в материалах к письму не обнаружено. Пересылать письмо другим пользователям **запрещено**
- **Спам** – это рассылка коммерческой и иной рекламы или подобных коммерческих видов сообщений лицам, не выразившим желания их получать

Инструкция пользователя РИС ПТО

Пользователю **запрещается**:

- Подключать к компьютеру **не зарегистрированные** машинные носители информации (флеш-накопители, съемные жесткие диски и т.д.)
- Сообщать иным лицам свои **пароли**, передавать **личные идентификаторы и ключевые носители**
- Хранить свои **пароли** в открытом виде в доступном другим пользователям месте, например, в виде наклейки на мониторе, под клавиатурой
- Самостоятельно **устанавливать/удалять программы** на компьютере. Установку/удаление может осуществлять только специалист службы поддержки пользователей после получения соответствующей заявки
- Самостоятельно **перемещать/переподключать** технику. Это могут производить только сотрудники службы поддержки. Также необходимо **оповестить** администратора безопасности о перемещении техники
- Предоставлять доступ к своему компьютеру лицам, **не допущенным** к работе в РИС ПТО
- Использовать электронную почту **сторонних сервисов** (например, gmail.com, yandex.ru и т.п.)
- Размещать для хранения на общих сетевых дисках, в том числе Disk_K, информацию **конфиденциального характера**, в том числе **Персональные данные**

Машинные носители информации (МНИ)

Согласно Приказу министерства по информатизации, связи и вопросам открытого управления Тульской области №83-осн от 30.10.2017:

- Служебные МНИ (flash-накопители, внешние жесткие диски, цифровые фотоаппараты и диктофоны) должны быть **зарегистрированы**
- **При наличии** на флеш-накопителе **наклейки** с учетным номером и ФИО администратора безопасности, он считается зарегистрированным
- **Запрещена** регистрация и использование **личных** МНИ
- Пользователь **обязан** обеспечить безопасность и конфиденциальность информации, содержащейся на МНИ
- **Уничтожение информации** на неисправном МНИ осуществляется специалистами ГАУ ТО «ЦИТ»
- В нерабочее время **ключевые носители информации** должны храниться в индивидуальных хранилищах, запираемых на замок (шкафах, ящиках, сейфах) или сдаваться на хранение лицу, назначенному ответственным за хранение съемных носителей, в опечатанном конверте (пенале) с фиксацией факта сдачи/выдачи в «Журнале выдачи съемных носителей информации»

Антивирусная защита

Согласно Приказу министерства по информатизации, связи и вопросам открытого управления Тульской области №109-осн от 27.08.2021:

- На рабочих местах пользователей установлен **антивирус** Dr.Web или Kaspersky Endpoint
- Ежедневно пользователь обязан **проверять наличие и работоспособность** антивируса. При его отсутствии/некорректной работе необходимо **незамедлительно сообщить** об этом в службу поддержки пользователей и администратору безопасности
- При обнаружении признаков **заражения** необходимо **отключить компьютер** от сети и **незамедлительно сообщить о заражении** администратору безопасности и в службу поддержки пользователей
- При необходимости подключения и последующей работы с МНИ, который использовался для передачи информации со сторонними организациями, **в обязательном порядке** проведите полную его **проверку** антивирусом

Парольная защита

Согласно Приказу министерства по информатизации, связи и вопросам открытого управления Тульской области №88-осн от 19.08.2019:

- **Заявка на предоставление доступа** новому пользователю оформляется за подписью руководителя организации, сотрудником которой является пользователь и направляется посредством АСЭД Дело в адрес оператора (ГАУ ТО «ЦИТ»)
- Обязательные **требования** к паролю от учетной записи:
 - длина пароля должна быть **не менее** 8 символов;
 - в числе символов пароля обязательно **должны присутствовать** буквы в верхнем и нижнем регистрах, цифры и (или) специальные символы (@, #, \$, *, % и т. п.);
 - пароль **не должен включать** в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций и т. д.), а также общепринятые сокращения и термины (user, qwerty, password, 123456 и т. п.);
 - при смене пароля новое значение **должно отличаться** от предыдущих, использованных ранее
- Смена паролей от учетных записей производится ежеквартально (через 90 дней)
- **Запрещено** хранение парольной информации на рабочем столе (на мониторе, под клавиатурой) и в местах, где его легко обнаружить. Хранение возможно **только** в закрывающемся ящике стола, личном сейфе
- **НИКОМУ НЕЛЬЗЯ СООБЩАТЬ ВАШ ПАРОЛЬ**

Wi-Fi

Согласно Приказу министерства по информатизации, связи и вопросам открытого управления Тульской области №90-осн от 20.07.2016:

- **Исключено** использование мобильных устройств связи и беспроводных точек доступа, в том числе беспроводных сетей, предоставляющих несанкционированный доступ к региональной защищенной сети передачи данных органов исполнительной власти Тульской области и аппарата правительства Тульской области
- Использование **мобильной точки доступа** (создание точки доступа Wi-Fi с использованием смартфона и других устройств) в пределах контролируемой зоны здания правительства Тульской области **ЗАПРЕЩЕНО**

Служебная электронная почта

Согласно Приказу министерства по информатизации, связи и вопросам открытого управления Тульской области №21-осн от 16.02.2016:

- Для обмена информацией между государственными органами, подведомственными учреждениями и органами местного самоуправления в качестве отправителей и получателей электронных сообщений используются только адреса электронной почты вида **tularegion.ru/tularegion.org**
- **Запрещено** использование электронных почт сторонних сервисов (gmail.com, yandex.ru, mail.ru и др.)
- **Запрещено** использование служебной электронной почты для обмена информацией, отнесенной к категории ограниченного доступа
- Если необходимо, чтобы коллега **отслеживал** Вашу рабочую почту и **отвечал** на письма, до того, как Вы уйдете в отпуск, свяжитесь с Вашим администратором безопасности или обратитесь в службу поддержки пользователей. Вам будут настроены правила переадресации, таким образом, на период, пока Вы находитесь в отпуске, письма, приходящие на Вашу почту, будут дублироваться и коллеге
- При получении на служебную электронную почту **подозрительных писем**, поступивших с незнакомого адреса, содержащих ссылки на скачивание файлов или вложение, переслать его как вложение на почтовый ящик servicedesk@tularegion.ru и spam@tularegion.ru с пометкой «*Прошу проверить на спам*». Переходить по ссылкам и скачивать вложения можно только **после** получения сообщения от специалиста о том, что вирусов в материалах к письму не обнаружено. Пересылать письмо другим пользователям **запрещено**

Удаленный доступ

- Если Вам поступает **звонок** с городского/мобильного телефона и звонящий представляется сотрудником службы поддержки пользователей:
 - уточните **цель** звонка;
 - попросите **перезвонить** с IP-телефона;
 - обязательно попросите его назвать фамилию, имя и **отправить** Вам личное сообщение через Microsoft Lync или Microsoft Outlook, чтобы удостовериться в личности звонящего.
- **Удаленный доступ** к вашему компьютеру разрешено предоставлять с помощью программ Microsoft Lync или Ассистент. При этом **запрещено** использовать TeamViewer или другое программное обеспечение удаленного администрирования.