**Раздел 1. Лекция 1. Конфиденциальность информации**

Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральным законодательством и принятыми в соответсвии с ним нормативными правовыми актами (информация ограниченного доступа).



К **общедоступной информации** относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. Общедоступная информация (например, что Солнце - это звезда, или что амурский тигр вымирающий вид, занесенный в Красную книгу) может использоваться любым человеком по своему усмотрению. А ограничения в отношении распространения такой информации могут устанавливаться только федеральными законами.

К **конфиденциальной информации** относится та информация, доступ к которой ограничен федеральными законами. Цели у ограничений разные. Например, защита основ конституционного строя, нравственности, здоровья, прав и законных интересов некоторых лиц, обеспечение обороны страны и безопасности государства. Конфиденциальность означает, что лицо, получившее доступ к определенной информации не имеет права передавать такую информацию другим лицам без согласия ее обладателя.

*Другими словами конфиденциальная информация это те сведения, доступ к которым ограничен нормативными актами.*

Государственный гражданский служащий, получивший доступ к конфиденциальной информации, несет персональную ответственность за соблюдение  установленных ограничений и  должен знать, какая именно информация относится к конфиденциальной, как правильно ее использовать и распространять.

Перечень сведений конфиденциального характера утвержден указом Президента Российской Федерации от 6 марта 1997 года № 188. Ознакомится с указом можно по [ссылке](http://www.kremlin.ru/acts/bank/10638).

К информации ограниченного доступа относятся:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

2. Сведения, составляющие тайну следствия и судопроизводства, сведения о лицах, в отношении которых в соответствии с федеральными законами от 20 апреля 1995 г. N 45-ФЗ "О государственной защите судей, должностных лиц правоохранительных и контролирующих органов" и от 20 августа 2004 г. N 119-ФЗ "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства", другими нормативными правовыми актами Российской Федерации принято решение о применении мер государственной защиты, а также сведения о мерах государственной защиты указанных лиц, если законодательством Российской Федерации такие сведения не отнесены к сведениям, составляющим государственную тайну.

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

7. Сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц, кроме сведений, которые являются общедоступными в соответствии с Федеральным законом от 2 октября 2007 г. N 229-ФЗ "Об исполнительном производстве".

С перечнем сведений, отнесенных к информации ограниченного доступа, можно ознакомиться, скачав прикрепленный к разделу файл.

**Раздел 1. Лекция 2. Служебная информация, ограниченного доступа**

Служебная информация — информация, касающаяся деятельности организации,не являющаяся общедоступной и ограничение на распространение которой диктуется служебной необходимостью.

Доступ к служебной информации может быть ограничен ее обладателем в рамках реализации полномочий, предусмотренных частью 3 статьи 6 Федерального закона от 27.07.2006 № 149-ФЗ "Об информации, информационных технолог относятся сведения, которыми обладают государственные органы и органы местного самоуправления в силу исполнения их служащими служебных обязанностей.

Доступ к такой информации ограничивается государственными органами и органами местного самоуправления соответствующими нормативными актами. Среди них можно выделить сведения, которые получены государственными органами в связи с предоставлением им информации гражданами (например, налоговая тайна), а также сведения, представляющие собой служебную информацию, распространение которой ограничено в силу служебной необходимости.

Таким образом, информация может являться служебной тайной, если она:

отнесена федеральным законом к служебной информации о деятельности государственных органов, доступ к которой ограничен по закону или в силу служебной необходимости;

является конфиденциальной информацией другого лица (коммерческая тайна, банковская тайна, секрет производства (ноу-хау), служебный секрет производства, персональные данные);

не является государственной тайной и не попадает под перечень сведений, составляющих государственную тайну;

получена представителем государственного органа или органа местного самоуправления только в силу исполнения обязанностей по службе в случаях и в порядке, установленных федеральным законодательством.

Для документов, содержащих служебную информацию ограниченного распространения, предусматривается специальный порядок обращения, касающийся, в частности, их приема, учета, хранения, уничтожения.

Вопросы использования такой информации регулируются Положением о порядке обращения со служебной информацией, утвержденным Постановлением Правительства РФ № 1233 от 3 ноября 1994 г. Указанным положением предусмотрена информация, которая не может быть ограничена в доступе:

нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, а также устанавливающие правовое положение организаций и полномочия госорганов, органов местного самоуправления;

информация, необходимая для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов;

сведения о структуре органа исполнительной власти, его функциях, направлениях и формах деятельности, а также его адреса;

порядок рассмотрения и разрешения заявлений и обращений граждан, а также юридических лиц и принятых по ним решений;

сведения о состоянии экономики и потребностей населения, об исполнении бюджета и использовании других государственных ресурсов;

документы, необходимые для реализации прав, свобод и обязанностей граждан, накапливаемые в открытых фондах библиотек, информационных системах организаций;

информация, содержащаяся в архивных документах архивных фондов (за исключением сведений и документов, доступ к которым ограничен законодательством Российской Федерации).

Как уже было отмечено, перечень служебной информации, отнесенной к информации ограниченного доступа, устанавливается самим государственным органом.

В Правительстве Приморского края, органах исполнительной власти Приморского края, структурных подразделениях аппарата Губернатора Приморского края и Правительства Приморского края (далее – государственные органы, подразделения) такой перечень утвержден постановлением Администрации Приморского края от 19.06.2017 № 237-па.

В соответствии с постановлением, к служебной информации, ограниченного доступа, относится следующая информация:

Вопросы промышленности и финансово-экономические вопросы организаций;

Вопросы оборонного комплекса;

Вопросы топливно-энергетического комплекса и жилищно-коммунального хозяйства;

Вопросы транспортного комплекса;

Вопросы агропромышленного комплекса;

Вопросы гражданской обороны;

Вопросы внешнеэкономической деятельности;

Вопросы проектирования, геодезии и картографии;

Вопросы информатизации, связи, защиты информации;

Вопросы безопасности и охраны;

Паспорта объектов религиозных организаций, подлежащих категорированию;

Сведения об организации контрольных мероприятий и проверок, проводимых в отношении органов исполнительной власти Приморского края и их подведомственных организаций;

Сведения конфиденциального характера, полученные Правительством Приморского края, аппаратом Губернатора Приморского края и Правительства Приморского края, органами исполнительной власти Приморского края от государственных органов, органов местного самоуправления муниципальных образований, организаций и несекретная переписка, связанная с рассмотрением указанных сведений.

С полным перечнем можно ознакомиться, скачав прикрепленный к лекции файл.

ВАЖНО! На практике следует руководствоваться подходом, что служебная информация является ограниченно распространяемой информацией, а служебная информация ограниченного доступа – ограниченно предоставляемой информацией.

**Раздел 2. Лекция 1. Персональные данные. Правила работы с персональными данными**

Определение персональных данных. Обработка персональных данных.

Почти все государственные органы исполнительной власти, подразделения обрабатывают персональные данные, например, в рамках подготовки ответов на обращения граждан, поступающих на регулярной основе в Правительство Приморского края.

Так как персональные данные относятся к защищаемой информации, законодательством Российской Федерации регулируются отношения, связанные с обработкой персональных данных, осуществляемой государственными органами власти, органами местного самоуправления, юридическими лицами и физическими лицами.

Должностным лицам, нарушившим требования законодательства Российской Федерации в области персональных данных , в зависимости от конкретных обстоятельств и серьезности деяния может грозить гражданско-правовая, дисциплинарная, административная и уголовная ответственность.

В соответствии с законом «О персональных данных» :

 персональные данные - любая информация, с помощью которой можно однозначно идентифицировать физическое лицо (субъект ПД).

К персональным данным относятся :

фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, состояние здоровья, почтовый адрес, номер телефона, информация, собираемая в интернете (IP-адресс, геопозиция, пол, сведения об используемых устройствах), фотография и другая информация, принадлежащая субъекту ПД.

Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 установлены следующие категории персональных данных:

Общедоступные

Специальная категория

Биометрические

Иные

Общедоступные персональные данные - данные, доступ к которым предоставлен неограниченному кругу лиц с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяются требования соблюдения конфиденциальности.

В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

Распространенным примером общедоступных персональных данных является телефонный справочник.

Специальная категория персональные данные - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

Биометрические персональные данные - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются для установления личности субъекта персональных данных.

Например, биометрическими персональными данными являются фотография или видео гражданина, отпечатки пальцев, отпечаток сетчатки глаза, образцы ДНК, результаты лабораторных и инструментальных исследований, медицинские снимки, заключения и анамнез и т.п.

Иные персональные данные - персональные данные, которые нельзя определить ни в одну из других групп.

Фактически, это дополнительная информация о человеке, которая часто меняется: размер зарплаты, социальный статус, рабочий стаж, длительность и даты отпуска и т. д.

В случае, если физическое или юридическое лицо, организация, государственный или муниципальный орган используют персональные граждан для выполнения возложенных на них функций, задач, в целях предоставления услуг и т.п. они являются операторами персональных данных и осуществляют обработку персональных данных.

Оператор персональных данных — 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.

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.

Важно отметить, что доступ и хранение тоже попадают под определение обработки. Таким образом, даже если сотрудник может только просматривать личные дела других сотрудников или организует хранение эти личных дела, это также считается обработкой персональных данных.

Обработка персональных данных может быть автоматизированной и без использования средств автоматизации.

Под автоматизированной обработкой персональных данных подразумевается осуществление обработки персональных данных с помощью средств вычислительной техники.

Обработка персональных данных без использования средств автоматизации (неавтоматизированная) - обработка персональных данных при непосредственном участии человека.

Чаще всего способы обработки различают так:

автоматизированная обработка персональных данных — обработка с использованием компьютера.

неавтоматизированная обработка — обработка персональных данных на бумажных носителях.

Зачастую возникают большие сложности в правильном определении какой именно вид обработки персональных данных осуществляется в государственных органах, подразделениях.

Дело в том, что почти во всех операциях по обработке ПД участвует человек, но это не значит, что обработка неавтоматизированная.

Примером неавтоматизированной обработки может стать выдача бумажного одноразового пропуска на территорию организации или талончика к врачу.

Под автоматизированной обработкой персональных данных понимается их обработка при помощи средств вычислительной техники.

Средствами вычислительной техники могут быть электронные вычислительные машины, комплексы и сети, вспомогательные и периферийные устройства, в том числе и установленное программное обеспечение.

Достаточно просто сохранить информацию в виде файла на компьютере – и обработка уже является автоматизированной.

Автоматизированная обработка персональных данных зачастую происходит с помощью информационных систем персональных данных.

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Однако, из Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» следует, что обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Отметим, что распространение в рамках неавтоматизированной передачи данных подразумевается также без средств вычислительнйой техники (принтеры, факты, сканеры), то есть если персональные данные были извлечены из системы, а потом распечатаны, то это уже автоматизированная обработка.

ВАЖНО!

Обработка персональных данных должна осуществляться на законной и справедливой основе и ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

Обработке подлежат только персональные данные, которые отвечают целям их обработки.

Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

**Раздел 2. Лекция 2. Правила работы с персональными данными**

Информация, обрабатываемая государственных органах, подразделениях в процессе служебной деятельности, может содержать (в виде информационных потоков, документов, файлов и баз данных, сообщений электронной почты, и т.д.) персональные данные граждан. Например, обращения граждан, направляемые в государственные органы, подразделения, содержат их персональные данные.

Обработка персональных данных должна производиться операторами (государственными органами, подразделениями) с соблюдением мер информационной безопасности.

Для защиты персональных данных по Федеральному закону от 26 января 2007 года № 152-ФЗ «О персональных данных» оператор должен предпринять ряд организационных и технических мер для того, чтобы персональные данные, переданные субъектом, всегда были доступны для обработки, не потерялись и не попали в руки посторонних.

У каждого оператора персональных данных должен быть разработан и утвержден документ, опеределяющий:

цели сбора и обработки персональных данных;

типы обрабатываемых персональных данных;

категории субъектов, персональные данные которых обрабатываются;

сроки их обработки и хранения;

порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований;

правила рассмотрения запросов субъектов персональных данных или их представителей;

правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;

 процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных.

Такой документ называется Политикой в отношении обработки и защиты персональных данных в государственном органе или подразделении (далее - Политика).

Политика необходима для обеспечения законных прав субъекта персональных данных и оператора. Каждый оператор обязан размещать уствержденную Политику в свободном доступе для ее ознакомления субъектом персональных данных.

Доступ к персональным данным могут иметь только уполномоченные лица государственного органа, подразделения, при этом указанные лица должны иметь доступ только к тем персональным данным , которые необходимы для выполнения конкретных задач и целей.

Список лиц, уполномоченных осуществлять обработку персональных данных, определяется в соответствии с перечнем должностей служащих государственного органа или подразделения, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным. Такой перечень утверждается руководителем государственного органа или подразделения, а лица, замещающие должности, установленные в перечни, должны обязательно с ним ознакомиться.

Помимо этого, государственные гражданские служащие, осуществляющие обработку персональных данных, должны быть ознакомлены с обязательством о немедленном прекращении обработки персональных данных, ставших известным ему в связи с исполнением должностных обязанностей, в случае расторжения с ним служебного контракта или трудового договора.

Оператор обязан собирать, обрабатывать и передавать данные куда-либо только с согласия их владельца.

Однако, законодательством предусмотрен ряд случаев, когда обработка персональных данных может осуществляться без согласия субъекта персональных данных. В государственных органах и подразделениях обработка персональных данных без согласия может осуществляться в следующих случаях

если обработка персональных данных необходима для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей. Например, рассмотрение и направление ответов гражданам в соответствии с Федеральным законом от 2.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

обработка персональных данных необходима для исполнения полномочий по предоставлению государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг", включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

обработка персональных данных, полученных в результате обезличивания персональных данных, осуществляется в целях повышения эффективности государственного или муниципального управления;

осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации;

обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством

обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о гражданстве Российской Федерации.

Остальные случаи обработки персональных данных без согласия субъекта персональных данных указаны в статьях 6 и 10 Федерального закона от 26 января 2007 года № 152-ФЗ «О персональных данных».

В каждом государственном органе, подразделении из числа государственных служащих органа, подразделения должен быть опеределен ответсвенный за организацию обработки персональных данных.

Такое лицо обязано осуществлять проверку соовтетсвия организации обработки персональных данных в органе, подразделении требованиям, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

Перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными органами утвержден Постановлением Правительства Российской Федерации от 21 марта 2012 года №211

**Раздел 2. Лекция 3. Способы передачи персональных данных**

В силу ст. 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

В Правительстве Приморского края передача персональных данных может осуществляться посредством:

Единой системы межведомственного электронного взаимодействия (СМЭВ);

федеральной информационной системы «Система межведомственного электронного документооборота» (МЭДО);

государственной информационной системы Приморского края «Региональная система межведомственного электронного документооборота»;

иных информационных систем персональных данных, защита информации в которых обеспечивается в соответствии с Составом и содержанием организационных и технических мер по обеспечению защиты персональных данных при их обработке в информационных системах персональных данных, утвержденным приказом ФСТЭК России от 18 февраля 2013 года № 21;

заказным письмом с уведомлением о вручении;

лично в руки с проставлением даты и номера входящего документа.

Запрещено передавать персональные данные по почте (служебной, личной), через мессенджеры и онлайн хранилища данных, облаков (Google Drive. Google Docs, Яндекс Диск, Next Cloud).

**Раздел 3. Лекция 1. Служебное автоматизированной рабочее место государственного служащего в Правительстве Приморского края**

Рабочее место может служить источником возникновения потенциальных угроз безопасности информации, так как большая часть информации обрабатывается с помощью компьютера. Чаще всего угрозы безопасности информации возникают вследствие незнания служащими правил защиты информации и (или) непонимание/ недопонимание необходимости их соблюдения.

Для уменьшения риска возникновения инцидентов информационной безопасности доступ пользователей к компонентам операционной системы и командам системного администрирования на рабочих местах в Правительстве Приморского края ограничен. Право на доступ к подобным компонентам предоставлено только системным администраторам и администраторам безопасности. Конечным пользователям предоставляется доступ только к тем командам, которые необходимы для выполнения их служебных обязанностей.

Государственные служащие обязаны знать и выполнять мероприятия по обеспечению информационной безопасности.

**Раздел 3. Лекция 2. Архивирование и резервирование**

Как уже было отмечено, почти вся информация обрабатывается с применением служебных автоматизированных рабочих мест государственных служащих, в следствии чего служебная информация хранится в памяти рабочих мест. Утеря информации может привести к приостановке деятельности государственного органа, подразделения, а ее полное восстановление не может быть гарантировано.

Чтобы избежать случайного или преднамеренного удаления информации, была придумана специальная процедура, которая позволяет дублировать все важные данные, – резервное копирование.

Резервное копирование – это копия данных, которая позволяет их восстановить в случае утраты или повреждения. Исходная информация после создания резервной копии не удаляется.

Основное назначение резервных копий — быстрое восстановление работоспособности систем в случае происшествий: поломка оборудования, ошибочные действия пользователей.

Резервный копии создаются для восстановления оперативной информации, с которой работает пользователь «здесь и сейчас». Однако, пользователь также имеет дело не только с оперативными данными - значительный объем многочисленных баз данных и файловых архивов содержат ретроспективную информацию.

Разницу между резервным копированием и архивированием данных проще всего описать на примере почтового ящика. Большинство пользователей используют для работы только те письма, что получены в последние несколько недель, но крайне неохотно удаляют старую переписку: она служит источником информации, с помощью которой можно «поднять» старые обсуждения, получить справочную информацию, восстановить полученные файлы. Иными словами — почта служит ценным источником ретроспективной информации.

Важно при создании архивных записей создать четкую структуру для быстрого поиска необходимой информации. Необходимо создать такой каталог с папками и документами который позволит искать нужную информацию с наименьшими затратами времени. Поэтому, рекомендуем на этапе работы с такими фалами сразу формировать отдельные папки по темам, чтобы затем просто добавить их в архив.

ВАЖНО!

Архивы не должны храниться вместе с остальными документами, задействованными в работе.

Создаваемые архивы должны быть защищены паролем.

Резервные копии и архивы могут создаваться путем дублирования файлов на отчуждаемые носители информации (USB-накопители, оптические диски, съемные жесткие диски), сетевые диски, облачное онлайн хранилище.

Для того, чтобы создать архив документов, защищенный паролем, необходимо использовать программы-архиваторы, установленные на компьютере.

…….

**Раздел 3. Лекция 3. Сетевые диски**

Сетевой диск — назначенный логический диск, который служит для хранения «общих» файлов, доступных для всех пользователей, на других персональных компьютерах, включенных в общую локальную сеть.

На каждом служебном автоматизированном рабочем месте государственного служащего в Правительстве Приморского края настроен сетевой диск.

В ситуациях, когда необходимо организовать совместный доступ государственных служащих из одного государственного органа, подразделения к данным или обеспечить их быструю передачу, необходимо использовать сетевой диск. Для каждого государственного органа, подразделения создана отдельная папка, куда могут обращаться государственные служащие.

Пересылка данных по служебной почте или с применением облачных хранилищ не гарантирует безопасность передаваемой информации.

…..

**Раздел 3. Лекция 4. Блокирование экрана рабочего места**

В процессе выполнения служебных обязанностей государственный служащий может покидать свое рабочее место и помещение, в котором оно расположено. Во время его отсутствия доступ в помещение могут получить посторонние лица, тогда информация, размещенная на экране рабочего стола, само рабочее место, а также документы, оставленные на столе, могут быть доступны для просмотра, их изменения, копирования и уничтожения.

Для нейтрализации угрозы несанкционированного доступа посторонних лиц к информации, размещенной на экране рабочего места, государственный служащий принимает меры по противодействию несанкционированному просмотру защищаемой информации с экрана монитора посторонними лицами.

К таким мерам относятся:

сворачивание окна, в котором отображена защищаемая информация или блокирование сеанса при нахождении посторонних лиц вблизи рабочего места с фронтальной стороны монитора;

ориентация монитора задней частью к дверным проемам и окнам. В случае вынужденной ориентации монитора фронтальной частью к окну, во время работы с защищаемой информацией шторы, жалюзи или рольставни закрываются.

блокирование сеанса.

Блокирование сеанса при котором блокируется экран монитора осуществляется путем одновременного нажатия сочетания клавиш «WIN» (между клавишами «Ctrl» и «Alt») и «L».

Для разблокировки автоматизированного рабочего места пользователю необходимо ввести свой пароль доступа.

Также необходимо обеспечить политику "чистого стола" в отношении бумажных документов. Носители (бумажные или электронные), когда они не используются, следует убирать и запирать (лучше всего в сейф или шкаф), особенно, когда помещение пустует.

ВАЖНО! По завершении рабочего дня, необходимо осуществлять полное выключение компьютера. Оставлять компьютер в спящем режиме можно только в исключительных случаях, согласованных с администраторами безопасности.

**Раздел 3. Лекция 5. Блокирование экрана рабочего места**

…..

**Раздел 3. Лекция 6. Угрозы безопасности при подключении к автоматизированному рабочему месту личных устройств, в том числе носителей информации**

….

**Раздел 4. Лекция 1. Безопасное использование служебных электронных сервисов**

**…..**

**Раздел 4. Лекция 2. Безопасность в сети «Интернет»**

**….**

**Раздел 4. Лекция 3. Использование служебного сервиса видеоконференц-связи**

**…..**

**Раздел 5. Лекция 1. Электронная подпись**