Тема 3. Информационные аспекты информационной безопасности. (2 часа)

Содержание:

1. Основы информации.
2. Информация с ограниченным доступом.
3. Реклама.
4. Владелец информации: информация государственная, коммерческая и личная.
5. Персональные данные. Авторское право.
6. Достоверность информации.
7. Основы шифрования.

ИНФОРМАЦИОННЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОСНОВЫ ИНФОРМАЦИИ

Согласно Федеральному закону от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» информация – это сведения (сообщения, данные) независимо от формы их представления.

Выделяют следующие категории информации:

Общедоступная информация, которая должна предоставляться свободно всем гражданам России;

ИНФОРМАЦИЯ С ОГРАНИЧЕННЫМ ДОСТУПОМ:

Являющаяся объектом гражданских прав. Это такая информация, обладатели которой вправе предоставлять доступ к ней по своему усмотрению, в частности на возмездной (платной) основе. Виды информации, являющейся объектом гражданских прав: произведения, являющиеся объектом авторского права; информация, являющаяся объектом патентного права; товарные знаки, знаки обслуживания и наименования мест происхождения товаров;

Конфиденциальная. Это такая информация, доступ к которой ограничивается в целях соблюдения интересов государства или прав и законных интересов их владельцев. К конфиденциальной информации относится государственная тайна, служебная и коммерческая тайны, а также тайны, связанные с правом на неприкосновенность личной жизни: персональные данные, личная и семейная тайны, тайна записи актов гражданского состояния, медицинская тайна и тайна вероисповедания.

Необходимо отметить, что имеет место быть информация нежелательного характера, которая содержит противозаконную, неэтичную и вредоносную информацию.

В Российской Федерации некоторые виды информации запрещены для распространения, в частности информация, пропагандирующая потребление и изготовление наркотиков, азартные игры, изготовление взрывчатых веществ, направленная на разжигание межнациональной розни, некоторые виды информации среди детей и отдельных возрастных групп и другая информация (подробная информация представлена в разделе «Актуальность информационной безопасности детей» данных методических рекомендаций).

Распространение данной информации преследуется по закону. В Российском законодательстве есть возможность в соответствии со статьями Кодекса об административных правонарушениях Российской Федерации и Уголовного кодекса Российской Федерации привлечь к административной и уголовной ответственности за распространение данной информации как владельцев сайтов, на которых размещается данная информация, так и ее авторов, и распространителей.

Неэтичная, противоречащая принятым в обществе нормам морали и социальным нормам, информация не запрещена к распространению, но может содержать информацию, способную оскорбить пользователей и оказать на них вредоносное воздействие, в частности манипулировать сознанием и действиями отдельных граждан или даже групп людей. Примером такой информации может стать нецензурная брань.

Изготовление и распространение подобной информации не попадает под действие Кодекса об административных правонарушениях Российской Федерации и Уголовного кодекса Российской Федерации, однако может повлечь санкции со стороны владельцев сайта, на которых пользователь размещает такую информацию, или со стороны организаций, имеющих возможность ограничить доступ к сайту, содержащего такую информацию.

Последний вид информации – вредоносный. Данный вид информации характеризуется тем, что распространяется данная информация для заражения компьютера вирусами, например, просмотр тех или иных видеоматериалов приводит к заражению компьютера вирусами. Заражение устройств позволяет злоумышленникам не только получить и украсть важные данные, но и дает им возможность манипулировать ими и действиями зараженного компьютера, в частности получить деньги незаконным способом (фишинг). Примером может стать распространение в сети «пиратского» программного обеспечения, установив которое пользователь может потерять доступ к операционной системе. Такие действия преследуются по закону в соответствии со статьями Уголовного кодекса Российской Федерации.

РЕКЛАМА

Особый вид информации – это реклама.

Согласно федеральному закону «О рекламе» реклама – это информация, распространенная любым способом, в любой форме и с использованием любых средств, адресованная неопределенному кругу лиц и направленная на привлечение внимания к объекту рекламирования, формирование или поддержание интереса к нему и его продвижение на рынке.

Потребители рекламы – это лица, на привлечение внимания которых к объекту рекламирования направлена реклама.

Реклама должна быть добросовестной и достоверной. Недобросовестная реклама и недостоверная реклама не допускаются.

Недобросовестной признается реклама, которая:

– содержит некорректные сравнения рекламируемого товара с находящимися в обороте товарами, которые произведены другими изготовителями или реализуются другими продавцами;

– порочит честь, достоинство или деловую репутацию лица, в том числе конкурента;

– представляет собой рекламу товара, реклама которого запрещена данным способом, в данное время или в данном месте, если она осуществляется под видом рекламы другого товара, товарный знак или знак обслуживания которого тождествен или сходен до степени смешения с товарным знаком или знаком обслуживания товара, в отношении рекламы которого установлены соответствующие требования и ограничения, а также под видом рекламы изготовителя или продавца такого товара;

– является актом недобросовестной конкуренции в соответствии с антимонопольным законодательством.

– Недостоверной признается реклама, которая содержит не соответствующие действительности сведения:

– о преимуществах рекламируемого товара перед находящимися в обороте товарами, которые произведены другими изготовителями или реализуются другими продавцами;

– о любых характеристиках товара, в том числе о его природе, составе, способе и дате изготовления, назначении, потребительских свойствах, об условиях применения товара, о месте его происхождения, наличии сертификата соответствия или декларации о соответствии, знаков соответствия и знаков обращения на рынке, сроках службы, сроках годности товара;

– об ассортименте и о комплектации товаров, а также о возможности их приобретения в определенном месте или в течение определенного срока;

– о стоимости или цене товара, порядке его оплаты, размере скидок, тарифов и других условиях приобретения товара;

– об условиях доставки, обмена, ремонта и обслуживания товара;

– о гарантийных обязательствах изготовителя или продавца товара;

– об исключительных правах на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридического лица, средства индивидуализации товара;

– о правах на использование официальных государственных символов (флагов, гербов, гимнов) и символов международных организаций;

– об официальном или общественном признании, о получении медалей, призов, дипломов или иных наград;

– о рекомендациях физических или юридических лиц относительно объекта рекламирования либо о его одобрении физическими или юридическими лицами;

– о результатах исследований и испытаний;

– о предоставлении дополнительных прав или преимуществ приобретателю рекламируемого товара;

– о фактическом размере спроса на рекламируемый или иной товар;

– об объеме производства или продажи рекламируемого или иного товара;

– о правилах и сроках проведения конкурса, игры или иного подобного мероприятия, в том числе о сроках окончания приема заявок на участие в нем, количестве призов или выигрышей по его результатам, сроках, месте и порядке их получения, а также об источнике информации о таком мероприятии;

– о правилах и сроках проведения основанных на риске игр, пари, в том числе о количестве призов или выигрышей по результатам проведения основанных

на риске игр, пари, сроках, месте и порядке получения призов или выигрышей по результатам проведения основанных на риске игр, пари, об их организаторе, а также об источнике информации об основанных на риске играх, пари;

– об источнике информации, подлежащей раскрытию в соответствии с федеральными законами;

– о месте, в котором до заключения договора об оказании услуг заинтересованные лица могут ознакомиться с информацией, которая должна быть предоставлена таким лицам в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации;

– о лице, обязавшемся по ценной бумаге;

– об изготовителе или о продавце рекламируемого товара.

– Реклама не должна:

– побуждать к совершению противоправных действий;

– призывать к насилию и жестокости;

– иметь сходство с дорожными знаками или иным образом угрожать безопасности движения автомобильного, железнодорожного, водного, воздушного транспорта;

– формировать негативное отношение к лицам, не пользующимся рекламируемыми товарами, или осуждать таких лиц;

– содержать информацию порнографического характера.

– В рекламе не допускаются:

– использование иностранных слов и выражений, которые могут привести к искажению смысла информации;

– указание на то, что объект рекламирования одобряется органами государственной власти или органами местного самоуправления либо их должностными лицами;

– демонстрация процессов курения и потребления алкогольной продукции;

– использование образов медицинских и фармацевтических работников, за исключением такого использования в рекламе медицинских услуг, средств личной гигиены, в рекламе, потребителями которой являются исключительно медицинские и фармацевтические работники, в рекламе, распространяемой в местах проведения медицинских или фармацевтических выставок, семинаров, конференций и иных подобных мероприятий, в рекламе, размещенной в печатных изданиях, предназначенных для медицинских и фармацевтических работников;

– указание на то, что рекламируемый товар произведен с использованием тканей эмбриона человека;

– указание на лечебные свойства, то есть положительное влияние на течение болезни, объекта рекламирования, за исключением такого указания в рекламе лекарственных средств, медицинских услуг, в том числе методов профилактики, диагностики, лечения и медицинской реабилитации, медицинских изделий.

В рекламе не допускается использование бранных слов, непристойных и оскорбительных образов, сравнений и выражений, в том числе в отношении пола, расы, национальности, профессии, социальной категории, возраста, языка человека и гражданина, официальных государственных символов (флагов, гербов, гимнов), религиозных символов, объектов культурного наследия (памятников истории и

культуры) народов Российской Федерации, а также объектов культурного наследия, включенных в Список всемирного наследия.

Не допускается реклама, в которой отсутствует часть существенной информации о рекламируемом товаре, об условиях его приобретения или использования, если при этом искажается смысл информации и вводятся в заблуждение потребители рекламы.

Не допускаются использование в радио-, теле-, видео-, аудио- и кинопродукции или в другой продукции и распространение скрытой рекламы, то есть рекламы, которая оказывает не осознаваемое потребителями рекламы воздействие на их сознание, в том числе такое воздействие путем использования специальных видеовставок (двойной звукозаписи) и иными способами.

Не допускается размещение рекламы в учебниках, учебных пособиях, другой учебной литературе, предназначенных для обучения детей по основным образовательным программам начального общего, основного общего, среднего общего образования, школьных дневниках, школьных тетрадях.

В целях защиты несовершеннолетних от злоупотреблений их доверием и недостатком опыта в рекламе не допускаются:

– дискредитация родителей и воспитателей, подрыв доверия к ним у несовершеннолетних;

– побуждение несовершеннолетних к тому, чтобы они убедили родителей или других лиц приобрести рекламируемый товар;

– создание у несовершеннолетних искаженного представления о доступности товара для семьи с любым уровнем достатка;

– создание у несовершеннолетних впечатления о том, что обладание рекламируемым товаром ставит их в предпочтительное положение перед их сверстниками;

– формирование комплекса неполноценности у несовершеннолетних, не обладающих рекламируемым товаром;

– показ несовершеннолетних в опасных ситуациях, включая ситуации, побуждающие к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью;

– преуменьшение уровня необходимых для использования рекламируемого товара навыков у несовершеннолетних той возрастной группы, для которой этот товар предназначен;

– формирование у несовершеннолетних комплекса неполноценности, связанного с их внешней непривлекательностью.

ВЛАДЕЛЕЦ ИНФОРМАЦИИ: ИНФОРМАЦИЯ ГОСУДАРСТВЕННАЯ, КОММЕРЧЕСКАЯ И ЛИЧНАЯ. ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Из вышеуказанного можно сделать вывод, что информация всегда имеет владельца.

В зависимости от вида собственности, информация может быть отнесена к информации государственной, коммерческой, личной (персональной):

– Перечень сведений, составляющих государственную тайну, формирует государство в лице его институтов и учреждений. Эти сведения являются обязательной тайной.

– Перечень сведений, определяющих коммерческую тайну, формируют организации самостоятельно. Он же обеспечивает их сохранность и защиту.

– Перечень своих персональных данных и личных (персональных) тайн определяет физическое лицо. Гражданин самостоятельно сохраняет и защищает эти данные.

Рассмотрим отдельно такую группу информации как персональные данные.

Персональные данные представляют собой информацию о конкретном человеке. Так согласно Федеральному закону от 27.07.2006 N 152-ФЗ «О персональных данных» персональные данные являются любой информацией, относящаяся к прямо или косвенно определенному или определяемому физическому лицу. Таким образом, персональные данные – это те данные, которые позволяют нам узнать человека в толпе, идентифицировать и определить как конкретную личность. Таких идентифицирующих данных огромное множество, к ним относятся: фамилия, имя, отчество, дата рождения, место рождения, место жительства, номер телефона, адрес электронной почты, фотография, возраст и пр.

Так, если мы кому-то скажем, свои фамилию, имя, отчество и адрес места жительства, то нас вполне можно будет опознать как конкретное лицо. Но если мы исключим из этого набора данных фамилию или адрес места жительства, то понять, о каком человеке идет речь, будет невозможно. Получается, что персональные данные - это не просто ваши фамилия или имя, персональные данные - это набор данных, их совокупность, которая позволяют идентифицировать вас.

В целом можно сказать, что персональные данные – это совокупность данных, которые необходимы и достаточны для идентификации какого-то человека.

К специальным персональным данным относятся: расовая или национальная принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья и пр.

Таким образом, специальные данные характеризуют наши взгляды, убеждения, мировоззрение, они определяют нашу социальную принадлежность к определенным группам. Например, человек может сказать: я демократ или я христианин.

По таким данным можно сформировать представление о человеке. Следует заметить, что приведенный перечень персональных данных не является исчерпывающим и может включать в себя еще множество иных идентификационных данных.

Биометрические персональные данные представляют собой сведения о наших биологических особенностях. Эти данные уникальны, принадлежат только одному человеку и никогда не повторяются. Биометрические данные заложены в нас от рождения самой природой, они никем не присваиваются, это просто закодированная информация о человеке, которую люди научились считывать. К таким данным относятся: отпечаток пальца, рисунок радужной оболочки глаза, код ДНК, слепок голоса и пр.

Персональные данные используются и обрабатываются организациями, например, социальными сетями, физическими лицами, например, при заказе услуг, и даже государством, например, при оказании государственных услуг.

Таким образом, персональные данные могут быть использованы как в коммерческих, так и некоммерческих целях.

Именно по этой причине перед получением персональных данных лица или организации (законодательством они объединены названием «Операторы

персональных данных»), которые хотят получить персональные данные, публикуют политику об обработке персональных данных, в которой отмечена цель их обработки, как они могут быть использованы, как соответственно удалены и другая информация.

Государство защищает право граждан в защите их права в области персональных данных и отдельно осуществляет защиту следующей информации о гражданах: не допускаются сбор, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей личную тайну, семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения.

Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации, в частности предусмотрена административная ответственность.

В этом контексте необходимо рассмотреть виды угроз конфиденциальности информации в целом:

- Разглашение — это умышленные или неосторожные действия владельца информации с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним. Разглашение может быть выражено в сообщении, передаче, предоставлении, пересылке, опубликовании, утере и в других формах обмена и действий с конфиденциальной информацией. Пример: гражданин потерял в поликлинике свою личную медицинскую карту, оставив ее в фойе поликлиники, в результате чего другие посетители поликлиники смогли ознакомиться с личной историей болезни гражданина.

- Утечка — это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она доверена по техническим каналам утечки информации. Пример: злоумышленник установил на WI-FI модем вирусную программу, позволяющую фиксировать все действия пользователя в сети «Интернет».

- Несанкционированный доступ - это овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам. Пример: компьютерный взлом социальной сети и кража персональных данных пользователей этой сети.

АВТОРСКОЕ ПРАВО

Одной из актуальнейших угроз информации личности, организаций и государства является защита интеллектуальной собственности в сети.

Термин "Интеллектуальная собственность" относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями.

Согласно статье 44 Конституции Российской Федерации каждому гарантируется свобода литературного, художественного, научного, технического и других видов творчества, преподавания.

Интеллектуальная собственность и отношения в данной области регулируются Гражданским кодексом Российской Федерации, в которых определены основные понятия.

Автором результата интеллектуальной деятельности признается гражданин, творческим трудом которого создан такой результат. Право авторства, право на имя и иные личные неимущественные права автора неотчуждаемы и непередаваемы. Отказ от этих прав ничтожен.

Исключительное право на результат интеллектуальной деятельности, созданный творческим трудом, первоначально возникает у его автора. Это право может быть передано автором другому лицу по договору, а также может перейти к другим лицам.

Гражданин или юридическое лицо, обладающие исключительным правом на результат интеллектуальной деятельности или на средство индивидуализации (правообладатель), вправе использовать такой результат или такое средство по своему усмотрению любым не противоречащим закону способом.

Другие лица не могут использовать соответствующие результат интеллектуальной деятельности или средство индивидуализации без согласия правообладателя.

Каждый из правообладателей вправе самостоятельно принимать меры по защите своих прав на результат интеллектуальной деятельности или на средство индивидуализации.

Интеллектуальные права на произведения науки, литературы и искусства являются авторскими правами. Автору произведения принадлежат следующие права:

- исключительное право на произведение;
- право авторства;
- право автора на имя;
- право на неприкосновенность произведения;
- право на обнародование произведения.

Автором произведения науки, литературы или искусства признается гражданин, творческим трудом которого оно создано. Лицо, указанное в качестве автора на оригинале или экземпляре произведения либо иным образом считается его автором, если не доказано иное.

Объектами авторских прав являются произведения науки, литературы и искусства независимо от достоинств и назначения произведения, а также от способа его выражения:

- литературные произведения;
- драматические и музыкально-драматические произведения, сценарные произведения;
- хореографические произведения и пантомимы;
- музыкальные произведения с текстом или без текста;
- аудиовизуальные произведения;
- произведения живописи, скульптуры, графики, дизайна, графические рассказы, комиксы и другие произведения изобразительного искусства;
- произведения декоративно-прикладного и сценографического искусства;

– произведения архитектуры, градостроительства и садово-паркового искусства, в том числе в виде проектов, чертежей, изображений и макетов;

– фотографические произведения и произведения, полученные способами, аналогичными фотографии;

– географические и другие карты, планы, эскизы и пластические произведения, относящиеся к географии и к другим наукам;

– другие произведения.

К объектам авторских прав также относятся программы для ЭВМ, которые охраняются как литературные произведения.

К объектам авторских прав относятся:

– производные произведения, то есть произведения, представляющие собой переработку другого произведения;

– составные произведения, то есть произведения, представляющие собой по подбору или расположению материалов результат творческого труда.

Авторские права распространяются как на обнародованные, так и на необнародованные произведения, выраженные в какой-либо объективной форме, в том числе в письменной, устной форме (в виде публичного произнесения, публичного исполнения и иной подобной форме), в форме изображения, в форме звуко- или видеозаписи, в объемно-пространственной форме.

Для возникновения, осуществления и защиты авторских прав не требуется регистрация произведения или соблюдение каких-либо иных формальностей.

Авторские права не распространяются на идеи, концепции, принципы, методы, процессы, системы, способы, решения технических, организационных или иных задач, открытия, факты, языки программирования, геологическую информацию о недрах.

Не являются объектами авторских прав:

– официальные документы государственных органов и органов местного самоуправления муниципальных образований, в том числе законы, другие нормативные акты, судебные решения, иные материалы законодательного, административного и судебного характера, официальные документы международных организаций, а также их официальные переводы;

– государственные символы и знаки (флаги, гербы, ордена, денежные знаки и тому подобное), а также символы и знаки муниципальных образований;

– произведения народного творчества (фольклор), не имеющие конкретных авторов;

– сообщения о событиях и фактах, имеющие исключительно информационный характер (сообщения о новостях дня, программы телепередач, расписания движения транспортных средств и тому подобное).

События и факты, содержащиеся в информационных сообщениях, не получают охраны по авторскому праву в силу того, что являются содержательной частью сообщения, тогда как авторское право охраняет форму произведения, а не его содержание.

Что касается самих сообщений, то они не охраняются авторским правом постольку, поскольку неоригинальны, представляют собой простое, механическое, нетворческое переложение событий и фактов, однако в случае, если форма выражения информационных сообщений является оригинальной, они являются объектом авторского права.

Срок действия авторского права распространяется в течение всей жизни автора и 70 лет после его смерти, однако право авторства, право на имя и право на защиту репутации автора бессрочны. Примером может стать произведение «Война и мир», которое перешло в статус общественного достояния после 70-летия с момента смерти Л.Н. Толстого.

Авторские права выступают в качестве гарантии того, что интеллектуальный и (или) творческий труд автора не будет напрасным, и дают ему справедливые возможности заработать на результатах своего труда, а также получить известность и признание.

Обладатель авторских прав для оповещения о своих правах вправе использовать знак охраны авторского права, который помещается на каждом экземпляре произведения и состоит из трех элементов:

– латинской буквы «С» в окружности: С (знак копирайта);
– имени (наименования) обладателя авторских прав;

Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в Интернете.

Обладатели авторских и смежных прав вправе требовать от нарушителя их права не только признания их права, но и в частности возмещение убытков, включая упущенную выгоду, и выплаты компенсации.

Важно, что нарушением авторского права является не только копирование и распространение, но и незаконное использование – чтение, прослушивание и просмотр.

Таким образом, пользователь должен соблюдать требования в области авторских прав, в частности использовать информацию:

– распространяемую бесплатно легально, зачастую при условии обязательного упоминания автора или источника, или на условиях просмотра рекламы, о чем указывается в правилах использования информации на сайте;
– распространяемая на основе свободной лицензии, примером которой является всемирная энциклопедия «Википедия».
– в повседневной жизни пользовать при использовании чужой информации при подготовке, например, статьи, доклада или поста в социальной сети должен указываться источник данной информации.

ДОСТОВЕРНОСТЬ ИНФОРМАЦИИ

В работе с информацией из любых источников необходимо помнить о необходимости проверки ее истинности, установление достоверности представленных фактов и сведений.

Специалисты определяют данный процесс термином «Верификация информации».

Основным механизмом проверки информации является критический анализ и восприятие информации, предполагающий изучение информации на предмет исторической верности, признаков субъективности и наличия признаков подделки.

Наиболее простой метод проверки информации – это перекрестная, то есть многократная проверка интересующей информации с использованием независимых источников.

Критика информации состоит из определения:

– времени и места появления информации или создания ее источника;

– автора текста или публикатора. Необходимо убедиться в компетентности автора, разбирается ли он в данном вопросе;

– полноты информации. Отвечает ли текст на ключевые вопросы: Что? Где? Когда? При каких обстоятельствах? Кто главные действующие лица?

– полнота доказательств. Какие доказательства использует автор? Видел ли он это сам или пересказывает чьи-то слова?

– надежность источников, поскольку одним из доказательств достоверности является наличие ссылок на источники. Важным критерием является наличие ссылок на официальные сайты органов власти или организаций. Если в качестве доказательства достоверности предоставляют фотографии или видео, то необходимо найти первоисточник и дату публикации изображения видео и соотнести с источником информации;

– изучение обстоятельств появления или публикации информации, а также цели создания этой публикации.

В противном случае, такая информация должна восприниматься не иначе, как авторский вымысел, и ей не нужно уделять большого внимания.

В конце отметим, что нельзя использовать Интернет как единственный источник информации, необходимо проверять информацию по другим источникам, особенно если эта информация касается жизненно важных моментов в жизни человека, например, здоровья, обучения, нормативно-правовых актов и других, поскольку в интернете не существует служб редакторов и корректоров, которые бы проверяли информацию на достоверность, корректность и полноту.

ОСНОВЫ ШИФРОВАНИЯ

Центральное место среди программно-технических средств безопасности занимает шифрование или криптография.

Криптографические методы защиты информации:

– шифрование;

– стеганография;

– кодирование;

– сжатие.

Процесс шифрования заключается в проведении обратимых математических, логических, комбинаторных и других преобразований исходной информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов. Исходными данными для алгоритма шифрования служат информация, подлежащая шифрованию, и ключ шифрования.

В настоящее время используются два основных метода шифрования – симметричное и асимметричное:

– В симметричном шифровании один и тот же ключ используется и для шифровки, и для расшифровки сообщений. Основным недостатком симметричного шифрования является то, что секретный ключ должен быть известен и отправителю, и получателю.

– В асимметричных методах применяются два ключа. Один из них, несекретный, используется для шифровки и может без всяких опасений передаваться по открытым каналам, другой – секретный – применяется для

расшифровки и известен только получателю. Асимметричные методы шифрования позволяют реализовать электронную подпись или электронное заверение сообщения.

В отличие от других методов криптографического преобразования информации, методы стеганографии позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации.

Содержанием процесса кодирования информации является замена смысловых конструкций исходной информации (слов, предложений) кодами. При кодировании и обратном преобразовании используются специальные таблицы или словари.

Сжатие информации может быть отнесено к методам криптографического преобразования информации с определенными оговорками. Целью сжатия является сокращение объема информации. В то же время сжатая информация не может быть прочитана или использована без обратного преобразования. Даже если держать в секрете алгоритмы, то они могут быть сравнительно легко раскрыты статистическими методами обработки. Поэтому сжатые файлы конфиденциальной информации подвергаются последующему шифрованию.

В целом шифрование возникло со времени появления письменности, когда возникла и получила свое дальнейшее развитие потребность в обеспечении стойкости отдельных сообщений, передаваемых почтовыми отправлениями. Первые шифротексты носили некоторый коммерческий характер. В дальнейшем стали шифроваться тексты медицинского характера, купли-продажи скота и недвижимости.

Активное проведение военных действий явилось мощным стимулирующим воздействием на разработку методов шифрования при передаче секретных сообщений. Так, в 56 году до н.э. во времена войны с галлами римский диктатор К. Цезарь при подчинении Риму заальпийской Галлии использовал в системе передачи секретных сообщений шифр замены. Идея шифра замены используется и в современных методах шифрования, так как является частным случаем отображения множества символов исходного текста на множестве символов зашифрованного текста. Шифрование, применявшееся К. Цезарем, осуществлялось следующим образом. Под символами греческого алфавита приписывался тот же алфавит, но сдвинутый по циклу на "n" позиций (в частности, К. Цезарь в письменности, которая дошла до наших времен, осуществлял сдвиг на три позиции). При шифровании исходного текста буквы открытого текста из верхней строки записи заменялись на буквы нижнего алфавита. В этом случае, ключом шифрования и дешифрования является число сдвигов нижней строки алфавита по отношению к верхней.

Шифрование и криптографию можно увидеть и в обычной жизни каждого человека.

Существуют персональные данные, которые представляют собой набор цифр, позволяющие определить конкретного человека. Такими персональными данными являются: номер и серия паспорта, страховой номер индивидуального лицевого счета (СНИЛС), индивидуальный номер налогоплательщика (ИНН), номер банковского счета, номер банковской карты. Такие «кодовые данные» представляют собой некий набор зашифрованной информации о человеке. Шифрование этих данных может производиться государством. Например, когда

ребенку исполняется 14 лет, ему выдают паспорт в ФМС. Такой паспорт содержит серию и номер, а также иную информацию.

Для подписания электронных документов также используются инструменты криптографического преобразования - Электронная цифровая подпись (ЭЦП).

ЭЦП может признаваться равнозначной собственноручной подписи лица и использоваться для подтверждения любой информации, передаваемой в электронном виде. Все экземпляры электронного сообщения, подписанного ЭЦП, имеют силу оригинала.

ЭЦП может использоваться физическими и юридическими лицами, органами государственной власти и органами местного самоуправления.

ЭЦП представляет собой последовательность символов, полученную в результате преобразования исходной информации с использованием закрытого ключа ЭЦП (последовательность символов, предназначенная для выработки ЭЦП и известная только владельцу).

Для получения ЭЦП гражданину или организации необходимо получить сертификат открытого ключа ЭЦП (сертификат ключа подписи) – это документ, выданный и заверенный специальным удостоверяющим центром, подтверждающий принадлежность ключа ЭЦП лицу.

Несовершеннолетние граждане имеют право на использование ЭЦП и получение сертификата ключа подписи.