Конфиденциальная информация

Вводная часть

На сегодняшнем занятии будет рассмотрено понятие «конфиденциальная информация», виды конфиденциальной информации, а также сформировано понимание того, какая информация относится к конфиденциальной, а какая не относится к конфиденциальной информации и что же необходимо защищать в области информационной безопасности.

Актуальность данного занятия определяется тем, что в настоящее время важной составляющей развития современных организаций или предприятий является автоматизация бизнес-процессов с использованием средств вычислительной техники и телекоммуникаций. Следствием этого является неуклонный рост объемов информации, которая подвергается обработке и накоплению в электронном виде.

С ростом электронного документооборота предприятия возрастает зависимость успеха его деятельности от непрерывности функционирования автоматизированной информационной системы (АИС) как единого целого и от сохранности корпоративной информации в процессе ее обработки и хранения на электронных носителях.

Повседневное использование информационных технологий становится обыденным и приводит к неосознанию конечности надежности техники, а в связи с этим существует вероятность отказа оборудования, приводящая к сбоям в доступе к электронной информации, а в худшем случае – к частичной или полной ее потере.

Развитие информационной системы, являющееся неотъемлемой частью успешного развития бизнеса, влечет за собой ужесточение требований к непрерывности ее функционирования, а также к сохранности и обеспечению конфиденциальности корпоративной информации, что в свою очередь втягивает предприятие во всю большую зависимость от уязвимости, постоянно усложняющейся АИС.

В ходе занятия будут рассмотрены следующие учебные вопросы:

1. Конфиденциальная информация.
2. Виды конфиденциальной информации.

Первый учебный вопрос: «Конфиденциальная информация»

В рассматриваемом ранее нами **Федеральном законе № 149 от 08.07.2006 г. «Об информации, информационных технологиях и о защите информации»** дано понятие **«конфиденциальной информации».**

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Одним из ***Принципов правового регулирования отношений в сфере информации, информационных технологий и защиты информации*** является:

2) установление ограничений доступа к информации только федеральными законами

5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите, содержащейся в них информации

7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

Статья 9. Ограничение доступа к информации.

1. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

2. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

2.1. Порядок идентификации информационных ресурсов в целях принятия мер по ограничению доступа к информационным ресурсам, требования к способам (методам) ограничения такого доступа, применяемым в соответствии с настоящим Федеральным законом, а также требования к размещаемой информации об ограничении доступа к информационным ресурсам определяются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

3. Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

4. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим государственную тайну, коммерческую тайну, служебную тайну и иную тайну (например, профессиональную тайну), обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

5. Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при

осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

6. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.

7. Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе.

8. Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

9. Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.

***Статья 16. Защита информации*.**

1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

2. Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

***Статья 17. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации*).**

1. Нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Для понимания вопросов конфиденциальности информации, необходимо изучить еще ряд документов.

Одним из них является **Федеральный закон № 187 «О безопасности критической информационной инфраструктуры Российской Федерации».**

Основными положениями данного закона являются понятия:

Критическая информационная инфраструктура - объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

Объекты критической информационной инфраструктуры - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

Безопасность критической информационной инфраструктуры - состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак.

Компьютерная атака - целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации;

Компьютерный инцидент - факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки.

Статья 4. Принципы обеспечения безопасности критической информационной инфраструктуры.

Принципами обеспечения безопасности критической информационной инфраструктуры являются:

1) законность;

2) непрерывность и комплексность обеспечения безопасности критической информационной инфраструктуры, достигаемые в том числе за счет взаимодействия уполномоченных федеральных органов исполнительной власти и субъектов критической информационной инфраструктуры;

3) приоритет предотвращения компьютерных атак.

Статья 5. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

2. *К силам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, относятся*:

1) подразделения и должностные лица федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

2) организация, создаваемая федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования

государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, для обеспечения координации деятельности субъектов критической информационной инфраструктуры по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты (далее - национальный координационный центр по компьютерным инцидентам);

3) подразделения и должностные лица субъектов критической информационной инфраструктуры, которые принимают участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак и в реагировании на компьютерные инциденты.

3. *Средствами, предназначенными для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, являются* технические, программные, программно-аппаратные и иные средства для обнаружения (в том числе для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры), предупреждения, ликвидации последствий компьютерных атак и (или) обмена информацией, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак, а также криптографические средства защиты такой информации.

Статья 7. Категорирование объектов критической информационной инфраструктуры.

1. Категорирование объекта критической информационной инфраструктуры представляет собой установление соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения.

Далее в Законе раскрываются вопросы категорирования ***объектов критической информационной инфраструктуры***, которые вы изучите самостоятельно

Задание на самостоятельную подготовку:

- изучить Федеральный закон № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» в полном объеме и быть готовым им руководствоваться в ходе учебного процесса.

Следующий документ, определяющий вопросы конфиденциальной информации, является **Указ Президента Российской Федерации № 188 от 6 марта 1997 года «Об утверждении перечня сведений конфиденциального характера»**.

Перечень сведений конфиденциального характера

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

3. Сведения, составляющие тайну следствия и судопроизводства, сведения о лицах, в отношении которых в соответствии с Федеральными законами от 20 апреля 1995 года № 45-ФЗ «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов» и от 20 августа 2004 года № 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.

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 года № 229-ФЗ «Об исполнительном производстве».

Таким образом, данный Указ определяет виды конфиденциальной информации, которые мы более подробно рассмотрим в следующем учебном вопросе.

На этом изложение первого учебного вопроса завершено.

Второй учебный вопрос: «Виды конфиденциальной информаций»

Рассмотренный в предыдущем вопросе «Перечень сведений конфиденциального характера» определяет следующие виды конфиденциальной информации:

- персональные данные;
- государственную тайну;
- коммерческую тайну;
- служебную тайну;
- иная тайна в соответствии с законодательством (например, врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

Рассмотрим содержание некоторых категорий.

Первая категория – «**персональные данные**».

Данная категория определена **Федеральным законом № 152 от 14 июля 2006 года «О персональных данных»**.

Настоящим Федеральным законом регулируются 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 органами, юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным (*часть в редакции, введенной в действие с 27 июля 2011 года Федеральным законом от 25 июля 2011 года N 261-ФЗ, распространяется на правоотношения, возникшие с 1 июля 2011 года*).

Действие настоящего Федерального закона не распространяется на отношения, возникающие при:

1) обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;

2) организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;

3) обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

Рассмотрим основные положения данного закона:

Статья 2. **Цель настоящего Федерального закона.**

Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Статья 3. **Основные понятия, используемые в настоящем Федеральном законе.**

В целях настоящего Федерального закона используются следующие основные понятия:

1) **персональные данные** – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

2) **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;

3) **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.

4) **распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

5) **предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Статья 5. **Принципы обработки персональных данных.**

2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

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

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

5. 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.

7. 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.

Статья 6. **Условия обработки персональных данных:**

1. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных настоящим Федеральным законом. Обработка персональных данных допускается в следующих случаях:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

3) обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;

3.1) обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве.

4) обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года № 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;

5) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по

которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

6) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

7) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц, в том числе в случаях, предусмотренных Федеральным законом «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях», либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

8) обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

9) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 настоящего Федерального закона, при условии обязательного обезличивания персональных данных;

9.1) обработка персональных данных, полученных в результате обезличивания персональных данных, осуществляется в целях повышения эффективности государственного или муниципального управления, а также в иных целях, предусмотренных Федеральным законом «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве» и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных», в порядке и на условиях, которые предусмотрены указанным Федеральным законом (*Пункт дополнительно включен с 1 июля 2020 года Федеральным законом от 24 апреля 2020 года N 123-ФЗ*);

10) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (*далее - персональные данные, сделанные общедоступными субъектом персональных данных*);

11) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом;

11.1) обработка персональных данных объектов государственной охраны и членов их семей осуществляется с учетом особенностей,

предусмотренных Федеральным законом от 27 мая 1996 года № 57-ФЗ «О государственной охране».

2. Особенности обработки специальных категорий персональных данных, а также биометрических персональных данных устанавливаются соответственно статьями 10 и 11 настоящего Федерального закона.

3. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение оператора)

4. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

5. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

Статья 7. **Конфиденциальность 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.

Статья 8. **Общедоступные источники персональных данных.**

1. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). 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, сообщаемые субъектом персональных данных.

2. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

Статья 11. **Биометрические персональные данные**.

1. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, в связи с проведением обязательной государственной дактилоскопической регистрации, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации.

Статья 19. **Меры по обеспечению безопасности персональных данных при их обработке.**

1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

2. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также

обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

3. Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

1) уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;

2) требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

3) требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Следующая категория – «**государственная тайна**».

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации (**федеральный закон Российской Федерации № 5485-1 от 21.07.1993 «О государственной тайне»**).

Степени секретности сведений (грифы секретности):

особой важности;

совершенно секретно;

секретно.

Перечень сведений, отнесенных к государственной тайне (*утв. Указом Президента РФ от 30 ноября 1995 г. N 1203*):

1) сведения в военной области;

2) сведения в области экономики, науки и техники;

3) сведения в области внешней политики и экономики;

4) сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму и в области обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты.

Не подлежат отнесению к государственной тайне и засекречиванию сведения:

о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;

о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;

о фактах нарушения прав и свобод человека и гражданина;

о размерах золотого запаса и государственных валютных резервах Российской Федерации;

о состоянии здоровья высших должностных лиц Российской Федерации;

о фактах нарушения законности органами государственной власти и их должностными лицами.

Должностные лица, принявшие решения о засекречивании перечисленных сведений либо о включении их в этих целях в носители сведений, составляющих государственную тайну, несут уголовную, административную или дисциплинарную ответственность в зависимости от причиненного обществу, государству и гражданам материального и морального ущерба.

Рассмотрим **содержание коммерческой тайны**.

Федеральным законом **Российской Федерации** № 98 от 29 июля 2004 г. «О коммерческой тайне» (*с изменениями и дополнениями от: 2 февраля, 18 декабря 2006 г., 24 июля 2007 г., 11 июля 2011 г., 12 марта 2014 г., 18 апреля 2018 г.*) определены следующие положения.

Коммерческая тайна – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду

Информация, составляющая коммерческую тайну – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны

Право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации принадлежит обладателю такой информации с учетом положений настоящего Федерального закона

Информация, составляющая коммерческую тайну, полученная от ее обладателя на основании договора или другом законном основании, считается полученной законным способом

Информация, составляющая коммерческую тайну, обладателем которой является другое лицо, считается полученной незаконно, если ее получение осуществлялось с умышленным преодолением принятых обладателем информации, составляющей коммерческую тайну, мер по охране конфиденциальности этой информации, а также если получающее эту информацию лицо знало или имело достаточные основания полагать, что эта информация составляет коммерческую тайну, обладателем которой является другое лицо, и что осуществляющее передачу этой информации лицо не имеет на передачу этой информации законного основания

Для **обозначения ценности конфиденциальной коммерческой информации** используются три категории:

- «коммерческая тайна - строго конфиденциально»;
- «коммерческая тайна - конфиденциально»;
- «коммерческая тайна».

Используется и другой подход к **градации ценности коммерческой информации:**

- «строго конфиденциально - строгий учет»;
- «строго конфиденциально»;
- «конфиденциально».

Режим «Коммерческая тайна» вступает в силу после выполнения следующих мер:

1. Определен перечень информации, составляющей коммерческую тайну.

2. Ограничен доступ к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка.

3. Организован учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана.

4. Урегулированы отношения по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров.

5. Нанесен на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включен в состав реквизитов документов, содержащих такую информацию, гриф «Коммерческая тайна» с указанием обладателя такой информации (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

1) содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и

об индивидуальных предпринимателях в соответствующие государственные реестры;

2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;

3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

5) о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

6) о задолженности работодателей по выплате заработной платы и социальным выплатам;

7) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

9) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

11) обязательность раскрытия которых или недопустимость ограничения доступа, к которым установлена иными федеральными законами.

Должностные лица несут ответственность в соответствии с законодательством Российской Федерации за неправомерное отнесение сведений к коммерческой тайне, а также за не отнесение сведений к коммерческой тайне в случаях, предусмотренных законодательством Российской Федерации.

Рассмотрим **содержание служебной тайны**.

Федеральным законом «О служебной тайне» (Проект № 124871-4) определены следующие положения.

Служебная тайна – это охраняемая законом конфиденциальная информация о деятельности государственных органов, организаций, доступ к которой ограничен в силу служебной необходимости.

Режим служебной тайны – совокупность правовых, организационных, технических и иных мер, принимаемых уполномоченными должностными

лицами органов государственной власти и организаций, обеспечивающих ограничения на распространение сведений, составляющих служебную тайну, и на доступ к этим сведениям.

Сведения, составляющие служебную тайну (служебная тайна) – конфиденциальные сведения, образующиеся в процессе управленческой деятельности органа или организации, распространение которых препятствует реализации органом или организацией предоставленных ему полномочий, либо иным образом отрицательно сказывается на их реализации, а также конфиденциальные сведения, полученные органом или организацией в соответствии с их компетенцией в установленном законодательством порядке.

Сведения, относящиеся к служебной тайне:

сведения, поступившие от физических и юридических лиц, других органов государственной власти и организаций, доступ к которым ограничен в соответствии с федеральными законами, при наличии на документах, содержащих эти сведения или сопроводительных документах грифа «Служебная тайна».

Не подлежат отнесению к служебной тайне сведения:

содержащиеся в законодательных и иных правовых актах, устанавливающих права, свободы, обязанности граждан и порядок их реализации, а также правовой статус органов государственной власти, органов местного самоуправления, организаций;

о чрезвычайных ситуациях, происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

в области экологии, метеорологии, демографии, эпидемиологии и санитарии, культуры, сельского хозяйства, о состоянии преступности и другие сведения, необходимые для обеспечения безопасности граждан и населения в целом;

о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, организациям и учреждениям;

о фактах нарушения прав и свобод человека и гражданина, нарушении законности должностными лицами органов государственной власти, органов местного самоуправления, организаций и учреждений;

об использовании органами государственной власти, органами местного самоуправления бюджетных средств, иных государственных и местных ресурсов, о состоянии экономики и потребностях населения, если иное не предусмотрено федеральным законом;

о размерах золотого запаса и государственных валютных резервах Российской Федерации;

о деятельности органов государственной власти и органов местного самоуправления, накапливаемые в информационных системах органов и организаций и представляющие общественный интерес или необходимые для

реализации прав, свобод и обязанностей граждан, а также содержащиеся в официальных изданиях, поступающих в фонды библиотек и архивов;

о состоянии здоровья лиц, занимающих государственные должности категории «А»;

сведения о деятельности органов государственной власти,» обязательные для размещения в информационных системах общего пользования в соответствии с законодательством Российской Федерации.

Руководители органов государственной власти несут ответственность в соответствии с законодательством Российской Федерации за неправомерное отнесение сведений к служебной тайне, а также за не отнесение сведений к служебной тайне в случаях, предусмотренных законодательством Российской Федерации.

На этом изучение учебного вопроса завершено.

Литература

1. Федеральный закон Российской Федерации №149 от 08.07.2006 г. «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон Российской Федерации № 187 от 26 июля 2017 года «О безопасности критической информационной инфраструктуры Российской Федерации».

3. Указ Президента Российской Федерации № 188 от 6 марта 1997 года «Об утверждении перечня сведений конфиденциального характера».

4. Федеральный закон № 152 от 14 июля 2006 года «О персональных данных».

5. Федеральный закон Российской Федерации № 5485-1 от 21.07.1993 «О государственной тайне».

6. Федеральный закон Российской Федерации № 98 от 29 июля 2004 г. «О коммерческой тайне».

7. Федеральный закон Российской Федерации № 124871-4 «О служебной тайне» (Проект).

Заключение

Из представленного учебного материала необходимо уяснить понятие конфиденциальной информации, и какие сведения относятся к конфиденциальной информации, а какие нет.

Доцент кафедры БИТ Д.Власкин