Приложение 2

Основы информационной безопасности

Основные понятия информационной безопасности

Прежде чем говорить об обеспечении безопасности персональных данных, необходимо определить, что же такое *информационная безопасность*. Термин "*информационная безопасность*" может иметь различный смысл и трактовку в зависимости от контекста. В данном курсе под **информационной безопасностью** мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести *неприемлемый ущерб субъектам информационных отношений*, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры .

Основные понятия информационной безопасности

ГОСТ "*Защита информации*. Основные термины и определения" вводит понятие **информационной безопасности** как состояние защищенности информации, при котором обеспечены ее *конфиденциальность*, доступность и *целостность*.

- **Конфиденциальность** – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.
- **Целостность** – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;
- **Доступность** – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

Основные понятия информационной безопасности

Угрозы информационной безопасности – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. **Атакой** называется попытка реализации угрозы, а тот, кто предпринимает такую попытку, - **злоумышленником**. Потенциальные злоумышленники называются *источниками угрозы*.

Угроза является следствием наличия **уязвимых мест или уязвимостей** в информационной системе. Уязвимости могут возникать по разным причинам, например, в результате непреднамеренных ошибок программистов при написании программ.

Угрозы можно классифицировать по нескольким критериям:

- по *свойствам информации* (доступность, целостность, конфиденциальность), против которых угрозы направлены в первую очередь;
- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, *поддерживающая инфраструктура*);
- по способу осуществления (случайные/преднамеренные, действия природного/техногенного характера);
- по расположению источника угроз (внутри/вне рассматриваемой ИС).

Основные понятия информационной безопасности

Обеспечение информационной безопасности является сложной задачей, для решения которой требуется *комплексный подход*. Выделяют следующие уровни защиты информации:

- **законодательный** – законы, нормативные акты и прочие документы РФ и международного сообщества;
- **административный** – комплекс мер, предпринимаемых локально руководством организации;
- **процедурный уровень** – меры безопасности, реализуемые людьми;

программно-технический уровень – непосредственно средства защиты информации.

Законодательный уровень является основой для построения системы защиты информации, так как дает базовые понятия *предметной области* и определяет меру наказания для потенциальных злоумышленников. Этот уровень играет координирующую и направляющую роли и помогает поддерживать в обществе негативное (и карательное) *отношение* к людям, нарушающим информационную *безопасность*.

ФЗ "Об информации, информационных технологиях и о защите информации"

В российском законодательстве базовым законом в области защиты информации является ФЗ "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года номер 149-ФЗ. Поэтому основные понятия и решения, закрепленные в законе, требуют пристального рассмотрения. Закон регулирует отношения, возникающие при:
осуществлении права на поиск, получение, передачу, производство и распространение информации;
применении информационных технологий;
обеспечении защиты информации.

Закон дает основные определения в области защиты информации. Приведем некоторые из них:

- **информация** - сведения (сообщения, данные) независимо от формы их представления;
- **информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
- **информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
- **обладатель информации** - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
- **оператор информационной системы** - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.
- **конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

ФЗ "Об информации, информационных технологиях и о защите информации"

В статье 3 Закона сформулированы принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации:

- свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
- установление ограничений доступа к информации только федеральными законами;
- открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
- равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
- обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
- достоверность информации и своевременность ее предоставления;
- неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
- недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

ФЗ "Об информации, информационных технологиях и о защите информации"

Вся *информация* делится на **общедоступную** и ограниченного **доступа**. К общедоступной информации относятся общеизвестные сведения и иная *информация*, *доступ* к которой не ограничен. В законе, определяется *информация*, к которой нельзя ограничить *доступ*, например, *информация* об окружающей среде или деятельности государственных органов. Оговаривается также, что *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. Обязательным является соблюдение конфиденциальности информации, *доступ* к которой ограничен федеральными законами.

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.

Закон выделяет 4 категории информации в зависимости от порядка ее предоставления или распространения:

- информацию, свободно распространяемую;
- информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
- информацию, распространение которой в Российской Федерации ограничивается или запрещается.

ФЗ "Об информации, информационных технологиях и о защите информации"

Закон устанавливает равнозначность электронного сообщения, подписанного электронной цифровой подписью или иным аналогом собственноручной подписи, и документа, подписанного собственноручно.

Дается следующее *определение* защите информации - представляет собой принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- своевременное обнаружение фактов несанкционированного доступа к информации;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- постоянный контроль за обеспечением уровня защищенности информации.

Таким образом, ФЗ "Об информации, информационных технологиях и о защите информации" создает правовую основу информационного обмена в РФ и определяет *права* и обязанности его субъектов.

Персональные данные

Необходимость обеспечения безопасности персональных данных в наше время - объективная реальность. Современный человек не может самостоятельно противодействовать посягательству на его частную жизнь. Возросшие технические возможности по сбору и обработке персональной информации, развитие средств электронной коммерции и социальных сетей делают необходимым принятие мер по защите персональных данных.

Рассмотрим несколько примеров из повседневной жизни, когда нарушаются *права* человека на *конфиденциальность* персональных данных. Бывает так, что при оформлении дисконтной карты в магазине *покупатель* указывает следующие сведения: фамилию, номер телефона, электронный *адрес*, а затем получает сообщения и письма совершенно из других магазинов, в которых даже никогда не бывал. То есть магазин без согласия покупателя передал его данные третьим лицам. Если газета печатает ФИО и суммы выигрыша победителей лотереи без их ведома, или ТСЖ вывешивает на подъезде списки должников и сумму их долга - это примеры "безобидных " утечек. *Кража* персональных данных может нанести правообладателю ощутимый материальный *ущерб*, если речь идет о кредитных картах или информации о сбережениях в банке. Злоумышленники, обладающие достаточными техническими знаниями, похищают реквизиты банковских карт (скиминг) или имитируют сайты финансовых учреждений, чтобы заставить пользователя показать свою личную информацию (фишинг). На самом деле зачастую даже трудно установить источник утечки персональных данных вследствие высокой информатизации современного общества.

Государство на законодательном уровне требует от организаций и физических лиц, обрабатывающих *персональные данные*, обеспечить их защиту. Законодательство Российской Федерации в области *защиты персональных данных* основывается на Конституции РФ, международных договорах Российской Федерации, Федеральном законе РФ от 27 июля 2006 г. N 152-ФЗ "О персональных данных", Федеральном законе от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" и других определяющих случаи и особенности обработки персональных данных федеральных законов.

Персональные данные

Целью российского законодательства в области *защиты персональных данных* является обеспечение защиты прав и свобод гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Законодательством регулируются отношения, связанные с обработкой персональных данных, осуществляемой государственными органами власти, органами местного самоуправления, юридическими лицами и физическими лицами.

Основополагающим законом в области *защиты персональных данных* является Федеральный закон "О персональных данных" №152, который был принят Государственной думой 8 июля 2006 года и вступил в силу с 26 января 2007 года. Закон определяет:

- основные понятия, связанные с обработкой персональных данных;
- принципы и условия обработки персональных данных;
- обязанности оператора персональных данных;
- права субъекта персональных данных;
- виды ответственности за нарушение требований ФЗ-№152;
- государственные органы, осуществляющие контроль за соблюдением требований ФЗ-№152.

Персональные данные

В соответствии с Законом **персональные данные** - любая *информация*, с помощью которой можно однозначно идентифицировать физическое лицо (субъект ПД). К персональным данным в связи с этим могут относиться фамилия, имя, отчество, год, месяц, дата и *место* рождения, *адрес*, семейное, социальное, имущественное положение, образование, *профессия*, доходы, другая *информация*, принадлежащая субъекту ПД.

Операторами персональных данных являются государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Обработка персональных данных – действия (*операции*) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Информационная система персональных данных (далее ИСПД) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств [7].

Регуляторами называются органы государственной власти, уполномоченные осуществлять мероприятия по контролю и надзору в отношении соблюдения требований федерального закона. В ФЗ "О персональных данных" установлены три регулятора:

- Роскомнадзор (защита прав субъектов персональных данных)
- ФСБ (требования в области криптографии)
- ФСТЭК России (требования по защите информации от несанкционированного доступа и утечки по техническим каналам).

Так как ФЗ "О персональных данных" является лишь основой правового обеспечения защиты ПД, его требования в дальнейшем были конкретизированы в актах Правительства РФ и Министерства связи, нормативно-методических документах регуляторов.

Категории персональных данных

ФЗ "О персональных данных" выделяет следующие категории персональных данных.

Общедоступные ПД - данные, *доступ* к которым предоставлен неограниченному кругу лиц с согласия субъекта ПД или на которые в соответствии с федеральными законами не распространяются требования соблюдения конфиденциальности. Общедоступные источники персональных данных создаются в целях информационного обеспечения (например, справочники и 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*, предоставленные субъектом персональных данных.

Важно отметить, что сведения о субъекте ПД могут быть в любое время исключены из общедоступных источников по требованию субъекта либо по решению суда или уполномоченных государственных органов.

Специальные категории ПД - *персональные данные*, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. Их обработка допускается только в следующих случаях:

- субъект ПД дал согласие в письменной форме на обработку своих персональных данных;
- персональные данные являются общедоступными;
- персональные данные относятся к состоянию здоровья субъекта ПД и получение его согласия невозможно, либо обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;
- обработка персональных данных членов (участников) общественного объединения или религиозной организации при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов ПД;
- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации или необходима в связи с осуществлением правосудия.

Категории персональных данных

Совместный приказ ФСТЭК, ФСБ и Министерства информационных технологий и связи РФ от 13 февраля 2008 года N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" определяет следующие **категории персональных данных**, которые обрабатываются в ИСПД:

- Категория 1 – *персональные данные*, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни.
- Категория 2 – *персональные данные*, позволяющие идентифицировать субъекта ПД и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1.
- Категория 3 – *персональные данные*, позволяющие идентифицировать субъекта ПД.
- Категория 4 – обезличенные и (или) общедоступные *персональные данные*.

Биометрические персональные данные – это сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его *личность*. Они могут обрабатываться только при наличии согласия в письменной форме субъекта ПД. Обработка биометрических персональных данных без согласия субъекта ПД может осуществляться в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, об оперативно - розыскной деятельности, о государственной службе, о порядке выезда из РФ и въезда в Российскую Федерацию, уголовно-исполнительным законодательством.

Определение биометрических данных в российском законодательстве предоставляет оператору персональных данных возможность принятия самостоятельного решения об отнесении тех или иных данных к биометрическим. Это породило немало споров. Рассмотрим пример с фотографией. С одной стороны, она характеризует физиологические особенности человека. Но человек с течением времени может сильно измениться или *злоумышленник* может подделать внешние признаки под законного субъекта. Так ли однозначно в данном случае установление личности? В настоящее время представители регуляторов подтверждают, что фотография и видеоизображения относятся к биометрическим данным.

Права субъекта персональных данных

Субъект персональных данных – это физическое лицо, которое может быть однозначно идентифицировано на основе персональных данных, то есть фактически тот, чьи данные необходимо защищать. Рассмотрим основные *права* субъекта ПД, установленные ФЗ-№152. Право субъекта персональных данных на доступ к своим персональным данным. Это предполагает право субъекта на получение сведений об операторе персональных данных и о том, какие ПД, относящие к этому субъекту, он обрабатывает, а также непосредственный доступ к этим ПД. Субъект вправе требовать от оператора уточнения ПД, их блокирования или уничтожения, если они устаревшие, неполные или не являются необходимыми для заявленной цели обработки. Доступ к своим ПД предоставляется субъекту(или его представителю) при обращении либо на основании запроса. Полученная информация может содержать следующие сведения:

- цель обработки ПД
- способы обработки ПД
- сроки обработки ПД
- перечень допущенных к обработке ПД лиц
- перечень обрабатываемых ПД и источник их получения
- сведения о возможных юридических последствиях обработки ПД для субъекта ПД.

Закон определяет случаи, когда данное право субъекта ПД ограничивается, например, если речь идет о безопасности страны, нарушении конституционных прав и свобод других лиц или оперативно-розыскной деятельности.

Права субъектов ПД при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации. В данном случае обработка осуществляется только при условии предварительного согласия субъекта. При этом важно отметить, что обработка признается осуществленной без согласия субъекта, если оператор не доказал обратное. Оператор обязан немедленно прекратить обработку ПД по требованию субъекта.

Права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных. Закон запрещает принятие решений в отношении субъекта ПД исключительно на основании автоматизированной обработки, если не получено его согласия в письменной форме или в случаях, предусмотренных федеральными законами. Право на обжалование действий или бездействия оператора. Если субъект ПД считает, что оператор обрабатывает его ПД ненадлежащим образом, то есть нарушает его права, он может обратиться в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке. Необходимо отметить, что субъект ПД имеет право на возмещение убытков и компенсацию материального вреда в судебном порядке.

Обязанности оператора персональных данных

Ранее мы рассмотрели понятие **оператора персональных данных** и действия, являющиеся **обработкой персональных данных** . Исходя из определения, можно сделать *вывод* о том, что все без исключения организации являются операторами ПД, так как они накапливают, собирают и обрабатывают информацию о своих сотрудниках в рамках Трудового кодекса РФ. Помимо этого многие организации собирают сведения о своих клиентах, подрядчиках, поставщиках и партнерах в рамках своей основной деятельности. Главными обязанностями оператора ПД является уведомление Роскомнадзора об обработке ПД и ,собственно, защита ПД.

Законом предусмотрены случаи, когда оператор не обязан уведомлять Роскомнадзор об обработке ПД:

если его связывают с субъектом трудовые отношения;

если между оператором и субъектом существует договор и данные необходимы для исполнения обязательств по нему;

если данные относятся к членам религиозных объединений и общественных организаций и обрабатываются в соответствии с учредительными документами и с законом.

если данные являются общедоступными;

если включают в себя только ФИО;

данные необходимы для однократного пропуска на территорию оператора или аналогичных целей;

если данные включены в федеральные автоматизированные информационные системы и государственные информационные системы персональных данных;

если данные обрабатываются без использования средств автоматизации в соответствии с законами РФ.

Важно отметить, что оговаривается обязанность оператора не передавать *персональные данные* третьим лицам.

При этом многие организации допускают ошибку в том, что если они не обязаны уведомлять уполномоченный орган об обработке ПД, то можно не выполнять обязанности, возлагаемые законом на операторов ПД. Такие действия являются противозаконными, однозначно трактуются как невыполнение требований законодательства и караются мерами, предусмотренными Законом.

Основные принципы обеспечения безопасности персональных данных

Принцип законности. Проведение защитных мероприятий должно быть согласовано с действующим законодательством в области информации, информатизации и защиты информации с применением всех дозволенных методов обнаружения и пресечения нарушений при работе с информацией.

Принцип максимальной дружественности и прозрачности. Противодействие угрозам безопасности информации всегда носит недружественный характер по отношению к пользователям и обслуживающему персоналу ИС, так как меры по защите информации всегда налагают ограничения на работу организационного и технического характера. Поэтому принимаемые меры должны максимально совмещаться с используемыми операционной и программно-аппаратной структурой ИС, а также должны быть понятны и оправданы для пользователей.

Принцип превентивности. Меры по защите информации и внедряемые СЗИ должны быть нацелены, прежде всего, на недопущение (пресечение) реализации угроз безопасности информации, а не на устранение последствий их проявления.

Принцип оптимальности и разумной разнородности. Для сокращения расходов на создание систем обеспечения безопасности должен осуществляться оптимальный выбор соотношения между различными методами и способами противодействия угрозам безопасности информации. Дополнительно внедряемые средства защиты должны дублировать основные функции защиты, уже используемые в программно-аппаратной среде ИС, и по возможности иметь другое происхождение, чем сама эта среда, что позволяет существенно затруднить процесс преодоления защиты за счет иной логики построения защиты.

Принцип адекватности и непрерывности. Решения, реализуемые системами защиты информации, должны быть дифференцированы в зависимости от важности защищаемой информации и вероятности возникновения угроз ее безопасности. Безопасность информации в государственных информационных системах должна обеспечиваться непрерывно в течение всего жизненного цикла систем.

Принцип адаптивности. Системы обеспечения информационной безопасности должны строиться с учетом возможного изменения конфигурации ИС, роста числа пользователей, изменения степени конфиденциальности и ценности информации.

Основные принципы обеспечения безопасности персональных данных

Принцип доказательности и обязательности контроля. Должны реализовываться организационные меры внутри сети и применение специальных аппаратно-программных средств идентификации, аутентификации и подтверждения подлинности информации. Должны обеспечиваться обязательность, своевременность и документированность выявления, сигнализации и пресечения попыток нарушения установленных правил защиты.

Принцип самозащиты и конфиденциальности самой системы защиты информации.

Принцип многоуровневости и равнопрочности. ИС должна реализовывать защиту информации на всех уровнях своей жизнедеятельности (технологическом, пользовательском, локальном, сетевом). Защита должна строиться эшелонировано, и иметь несколько последовательных рубежей таким образом, чтобы наиболее важная зона безопасности находилась внутри других зон. Все рубежи защиты должны быть равнопрочными к возможности реализации угрозы.

Основные принципы обеспечения безопасности персональных данных

Принцип простоты применения и апробированности защиты. Должны применяться средства защиты, для которых формально или неформально возможно доказать корректность выполнения защитных функций, проверить согласованность конфигурации различных компонентов, а их применение пользователями и обслуживающим персоналом должно быть максимально простым, чтобы уменьшить риски, связанные с нарушениям правил их использования. По той же причине целесообразно использовать средства защиты информации, допускающие возможность централизованного администрирования.
Принцип преемственности и совершенствования. Система защиты информации должна постоянно совершенствоваться на основе преемственности принятых ранее решений и анализа функционирования ИС.
Принцип персональной ответственности и минимизации привилегий для пользователей всех уровней. Принимаемые меры должны определять права и ответственности каждого уполномоченного лица. Распределение прав и ответственности должно в случае любого нарушения позволять определить круг виновных. Система обеспечения информационной безопасности должна обеспечивать разделение прав и ответственности между пользователями.

Спасибо
за внимание!