Тип работы: Научно-исследовательская работа

Предмет: Информационное право

Введение

Актуальность исследования. В настоящее время привлекает внимание вопрос об анализе изучения политики государства в сфере информационных технологий на развитие российского общества. Происходит переход к массовым коммуникациям при взаимодействии власти на разных уровнях. Это ставит задачу комплексного изучения государственного управления информационными технологиями. При этом в информационной сфере оказываются персональные данные личности. Несколько раз по центральным средствам массовой информации передавались сообщение о неправомерном доступе злоумышленников к персональным данным, в результате чего был причинен ущерб правам и законным интересам государству и обществу, в связи с неправомерным доступом к персональным данным. В связи с этим на государство возлагается обязанность по защите персональных данных граждан.
Объектом исследования выступает информационная система персональных данных (ИСПДН).
Предметом курсовой работы выступают порядок защиты Защита информационной системы персональных данных (ИСПДН)
Цель работы состоит в анализе порядка защиты информационной системы персональных данных (ИСПДН)
Для достижения поставленной цели необходимо решить ряд взаимосвязанных задач в соответствии с практическим заданием.
Методология исследования вкачает методы научного познания, анализа, синтеза¸ сравнительно правовой и формально-юридический метод.

1) Установить вид ИСПДН
ПДн сотрудников, структура автономная, субъекты не сотрудники , более 100 000, то есть физические лица.
Субъектами, обязанными соблюдать конфиденциальность и целостность персональных данных, считаются:
а) субъекты специального оператора, иные лица, получившие доступ по соглашению с оператором;
б) любым другим гражданам, юридическим лицам, которым в силу определенных обстоятельств стали известны персональные данные других лиц, независимо от воли уполномоченного лица.
Операторами являются государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и/или осуществляющее обработку персональных данных, а также определяющее цели и содержание обработки персональных данных. Если оператор назначает обработку персональных данных другому лицу на основании договора, существенным условием договора является обязанность

обеспечивать конфиденциальность персональных данных и безопасность персональных данных при их обработке. .
Оператор выполняет свои функции в пределах полномочий, определенных специальными правовыми актами.
Следует признать, что "правовые режимы регулируют обычный правовой статус объектов права и предусматривают исключения из общего правила. Исключительность правового режима может быть определена непосредственно в законе... но даже если нет таких прямых указаний, исключительность может следовать из смысла закона. Я считаю, что конфиденциальность персональных данных является доминирующей, и исключение режима публичной доступности персональных данных и режима государственной тайны. Это неслучайно в пункте 2 статьи. 8 Закона "О персональных данных" предусматривает, что сведения о предмете персональных данных могут быть исключены из общедоступных источников персональных данных в любое время по требованию субъекта персональных данных или по решению суда или иных уполномоченных государственных органов. Этот закон также устанавливает меры по обеспечению безопасности персональных данных при их сборе, обработке для установления (подтверждения) режима.
Персональные данные могут быть отражены в отдельном документе, таком как паспорт, справка с места работы, или включены в документ, содержащий сведения, составляющие профессиональную тайну, такие как договор юридической помощи с адвокатом, договор банковского вклада с банком .
Персональные данные - это любая информация, относящаяся к конкретному лицу или информации, определенной этим лицом, включая его фамилию, имя, отчество, год, месяц, дату и место рождения, адрес, семью, социальное, имущественное положение, образование, профессию, доход, другую информацию. Например, другой информацией (персональными данными) будет информация о книгах, выбранных считывателем, которые собираются в базе данных библиотеки с помощью электронной формы заказа и карточек библиотеки штрих-кодов. Биометрические персональные данные (сведения, описывающие физиологические характеристики человека и на основании которых может быть установлена его личность) включают отпечатки пальцев, результаты анализа ДНК, сетчатки, атавизмы, различные нарушения развития и т. д.
Представляется, что право на конфиденциальность и целостность персональных данных содержит право требовать от третьих лиц не нарушать конфиденциальность персональных данных, предоставлять соответствующую информацию (его часть) другим лицам, для определения содержания и судьбы персональных данных, которые в силу определенных обстоятельств стали известны третьим лицам, в пределах, установленных законом .
Содержание права на неприкосновенность частной жизни и неприкосновенность персональных данных отражены в Законе о персональных данных, который предусматривает, что гражданин имеет право:
а) предоставлять свои персональные данные третьим лицам;
б) согласие на обработку персональных данных, отзыв согласия на обработку;
в) получать информацию об операторе, его местонахождении, персональных данных оператора относительно соответствующего субъекта персональных данных;
г) получить доступ к вашим персональным данным; д) требовать указания своих персональных данных, их блокировки или уничтожения в установленных случаях .
Возможность предоставления ваших персональных данных третьим лицам заключается в том, что определенная информация предоставляется гражданином по его просьбе как контрагента при заключении гражданско-правовых договоров. Таким образом, согласно договору на предоставление услуг доступа в интернет, провайдер получает информацию о пользователе. При заключении договора на оказание услуг местного телефонного гражданина в тексте договора с оператором указываются дата и место рождения, место жительства, паспортные данные и т.д.
Организационно-технические возможности сбора информации о пользователе (IP-адрес, количество и время посещений) являются владельцами интернет-ресурсов, которые посещает пользователь. Чтобы легализовать использование этой информации, как правильно отмечено в юридической литературе, владелец сайта должен получить максимально возможное подтверждение от лица, о котором собрана информация. В частности, сайт может быть размещен заметным и понятным с точки зрения описания использования информации владельцем сайта, а также обеспечения того, чтобы посетитель не мог получить доступ к контенту сайта без нажатия кнопки, подтверждающей согласие посетителя на сбор и использование информации о нем. .
Ряд законов предусматривает, что гражданин должен передавать информацию о себе в органы

государственной власти. В Австралии Управление Комиссара по вопросам конфиденциальности насчитало 187 информационных банков, управляемых различными государственными учреждениями для граждан. Досье содержит сведения о доходах, налогах, религии, политических взглядах, контактах, истории болезни и даже личности авторов писем, направленных премьер-министру. Глава службы считает, что такое досье можно использовать как во благо, так и во вред.
Гражданин предоставляет сведения о себе при заключении трудового договора (статьи 57, 65, 86 ТК РФ). В соответствии с Федеральным законом "О государственной гражданской службе Российской Федерации", государственный служащий обязан в установленном порядке предоставлять сведения о себе и членах семьи, предусмотренные Федеральным законом, а также сведения о полученных им доходах и имуществе, которые принадлежат ему для налогообложения, об обязательствах имущественного характера. Налоговый кодекс Российской Федерации обязывает отдельных налогоплательщиков представлять налоговые декларации, содержащие сведения о облагаемых налогом статьях, полученных доходах, понесенных расходах и т.д.
Некоторая информация собирается независимо от воли гражданина без предварительного уведомления, но в соответствии с федеральными законами. В России федеральный закон "Об оперативно-розыскной деятельности" предусматривает, что органы, осуществляющие оперативно-розыскную деятельность, применяют такие меры, как опрос граждан, опрос, отбор проб для сравнительного исследования, наблюдения и т.д. В процессе этой деятельности и ее результатах государственные органы становятся обладателями информации, составляющей тайну частной жизни граждан.
В последнее время наблюдается возрастание роли информатизации, развитие предоставления услуг, в том числе и государственных, что требует внесения персональных данных операторам. В связи с этим возрастает и необходимость обеспечения надлежащей защиты указанных персональных данных. Правовые основы защиты персональных данных предусмотрены федеральным законом «О персональных данных» и Указом Президента об отнесении информации к персональным данным, и утверждении перечня конфиденциальной информации , а так же нормативными актам в банковском секторе и иными нормативными актами. Предусмотрена ответственность за незаконное распространение и разглашение персональных данный вплоть до уголовной.
При этом на государственном уровне особенно охраняются персональные данные составляющие личную и семейную тайну.
Лица, осуществляющие доступ к персональным данным в силу характера своей деятельности несут персональную ответственность за нарушение конфиденциальности указанной информации.
При том, что законодательством прямо не предусмотрена ответственность за нарушение порядка сбора и хранения информации содержащейся на индивидуальных лицевых счетах в системе индивидуального персонифицированного учета пенсионного страхования, в связи с этим ответственность наступает по общим основаниям.
В деятельности правоохранительных органом зачатую встречаются случаи связанные с незаконным перехватом сообщений или незаконного перехвата персональных данных. В данном случае нарушаются права на защиту персональных данных, что является основанием для обращения с заявлением в уполномоченные органы и привлечения к ответственности руководителей организаций допустивших незаконную утечки информации, содержащей персональные данные, а так же самих сотрудников, допустивших такую утечку .
Нарушение права на личную неприкосновенность и неприкосновенность персональных данных проявляется либо в разглашении тайны, передаче этой информации третьим лицам без согласия уполномоченного лица, либо на расстоянии, изменении или блокировании персональных данных.
Российская Федерация справедливо заявляет, что "право на неприкосновенность частной жизни закреплено в статье 23 Конституции Российской Федерации , относится к особой роли индивидов в их отношениях с обществом и обществом. Она неразрывно связана с понятиями жизни, равенства, свободы и целостности личности. Это означает, что поиск оптимальных моделей взаимодействия между государством и индивидом, а также людьми между собой долгое время был долгой проблемой.

2) Изучить постановления правительства РФ №1119 о защите персональных данных (2012 год).
Угроза 1-го типа.
а) Вид персональных данных определить в соответствии с федеральным законом №152 о персональных данных.
Защита персональных данных граждан. Все граждане страны, а также другие граждане. В результате они

получают сведения о конкретном человеке, начиная с простейших (сведения о болезнях, верованиях, доходах, имуществе и т. д.). Гражданин не хочет, чтобы информация о нем стала известна широкому кругу людей. Для защиты всей этой информации используется специальный режим персональных данных . Обработка этих видов персональных данных регулируется специальными правилами.
Совокупность таких данных в научной литературе называется "высокочувствительными личными данными". В. Ивановский отмечает, что содержание таких данных зависит от национальных мнений, религиозных предпочтений, убеждений, членства в профессиональных объединениях, общественных и иных общественных организациях, от состояния здоровья., от особенностей сексуального поведения, от приговоров, приговоров и казней по уголовным делам.
Согласно закону N 152-ФЗ, публикуются персональные данные, не требующие решения по закону о защите прав. Эта ситуация подверглась критике со стороны некоторых авторов. Так, Н. Петрикина отметил, что неясно, как это должно делаться на практике. Более того, продолжающееся использование публичных персональных данных без согласия субъекта персональных данных, за исключением того, для чего они были опубликованы, противоречит установленному материальному условию в статье 6 Закона о согласии субъекта персональных данных на обработку его персональных данных.
Принимая во внимание специфику вопросов, направленных на защиту персональных данных и конфиденциальность, скоординированные действия и обеспечение международного сотрудничества между властями различных государств. Отметим, что ряд российских государств уже подписали меморандумы о сотрудничестве в защите прав субъектов персональных данных (Молдавия, Киргизия, Армения, Македония). Сейчас подписаны соглашения с Украиной, проводятся консультации, достигнуты договоренности с Боснией и Герцеговиной, а также с Хорватией. Это позволит значительно улучшить защиту прав граждан в будущем, в том числе за пределами РФ.
Кроме того, представители России принимают активное участие в международных акциях иного формата, в частности, согласно проекту соглашения между Россией и Евроюстом, а также в переговорах по проекту соглашения об оперативном сотрудничестве между Россией и Европолом и т. д.
Не технологические положения Конвенции защищают от вмешательства в частную жизнь государства и частных организаций, но сейчас они не отражают нынешний уровень правоотношений. На 29-м пленарном заседании Комитета сторон Конвенции Совета Европы о защите физических лиц при практической обработке персональных данных, состоявшемся в Страсбурге 27-30 2012 ноября, обсуждались предложения Совета европейских государств-членов по внесению поправок в ключевые положения Конвенции подряд. В частности, следует отметить, что предлагаемые положения статьи 12 предусматривают возможность передачи персональных данных получателя, находящегося под юрисдикцией международной организации или государства, которое не является участником Конвенции и не обеспечивает надлежащего уровня защиты персональных данных в определенных случаях. Эта передача является законным общественным интересом и необходимой мерой в демократическом обществе .
Также предлагается установить обязанность каждой стороны обеспечивать информирование компетентного надзорного органа об условиях передачи данных и предоставлять право надзорному органу требовать от лица передачи или получения персональных данных, принимаются доказательства эффективности и качества той или иной меры.
Большое внимание уделяется предложениям о принципах функционирования, правах и обязанностях этих надзорных органов, отвечающих за соблюдение принципов Конвенции в рамках национального законодательства государств-участников, начиная с Конвенции № 108. была принята более 30 лет назад и информационные технологии, используемые для передачи персональных данных, разрабатывались, менялись современные звонки и угрозы в связи с растущими возможностями использования огромных объемов конкретных персональных данных и т.д.

b) На оснований исходных данных о ИСПДН, установить уровень защищенности ИСПДН.
Персональные данные физических лиц - работников
5 декабря 2016 года Указом Президента Российской Федерации № 646 была утверждена "Доктрина информационной безопасности Российской Федерации" , раскрывающая официальные взгляды на обеспечение национальной безопасности в информационной сфере.
Также примечателен проект постановления правительства РФ "Об утверждении Положения о государственном контроле и надзоре за соответствием обработки персональных данных требованиям законодательства РФ", регламентирующий порядок государственного контроля в сфере обработки персональных данных.

Рассмотрим эти правовые акты через призму государственного контроля (надзора) в информационной сфере баланса между неприкосновенностью частной жизни человека и защитой интересов общества и государства.
Нормативным документом, раскрывающим Стратегию национальной безопасности РФ в информационной сфере, является доктрина информационной безопасности № 6465, нормы которой должны учитываться при принятии законодательства в этой сфере с точки зрения баланса между государственными и частными интересами. Между тем Информационная доктрина регулирует важнейшие социальные отношения, связанные со стратегическими целями и основными направлениями обеспечения информационной безопасности государства.
В связи с исключительной важностью этих правоотношений в современную эпоху считаем целесообразным рассмотреть уровень их регулирования - от подчиненного нормотворчества до уровня правотворчества. В этом случае мы можем избежать конфликта в понимании приоритета целей обработки персональных данных - защиты общественных интересов или защиты частной жизни как национальных интересов.
Другим нормативным правовым актом, устанавливающим дополнительные меры по противодействию терроризму и обеспечению общественной безопасности в информационной сфере, является антитеррористический закон Яровой . Его основные задачи: во-первых, расширение полномочий правоохранительных органов; во-вторых, введение новых требований к операторам связи и интернет-проектам; в-третьих, усиление регулирования религиозного контроля и надзора за соответствием обработки персональных данных требованиям Федерального закона "О персональных данных".
Государство установило обязанности операторов и организаторов распространения информации в интернете в соответствии с Федеральным законом от 6 июля 2016 года № 374-ФЗ. Статьи 15 и 64 настоящего Закона обязывают операторов связи и организаторов распространения информации в сети Интернет с 1 июля 2018 года хранить текстовые сообщения пользователей услуг связи, голосовую информацию, изображения, звуки, видео- и иные сообщения пользователей на территории Российской Федерации. Срок такого хранения может составлять до шести месяцев с даты завершения их получения, передачи, доставки или обработки. Информация о фактах приема, передачи, доставки и/или обработки речевой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услуг связи хранится операторами связи и организаторами распространения информации в сети Интернет в течение трех лет - в течение одного года после окончания таких действий.
Помимо хранения такой информации операторами связи и организаторами распространения информации в сети Интернет, последние обязаны предоставлять эту информацию уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечивающим безопасность РФ.
Данные положения, по нашему мнению, противоречат подпункту "а" пункта 8 Доктрины информационной безопасности Российской Федерации от 05.12.2016 № 6466, где обеспечение и защита частной жизни как конституционного права являются национальными интересами в информации, а также подпункт 1 пункта 1 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" в части получения согласия на обработку персональных данных. Иными словами, национальные интересы в информационной сфере - это не противодействие терроризму и обеспечение общественной безопасности, а защита неприкосновенности информационной стороны частной жизни граждан. Между тем террористические и экстремистские организации широко используют деструктивные информационные механизмы для воздействия на человеческое и общественное сознание в целях нанесения ущерба критически важной информационной инфраструктуре (пункт 13 Доктрины). В этой связи необходимо обеспечить баланс между необходимостью свободного обмена гражданами информацией и ограничениями, касающимися национальной безопасности.
В настоящее время Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) является органом исполнительной власти, осуществляющим государственный контроль и надзор в информационной сфере. При изучении вышеуказанных проблем должен был произойти научный разрез, прежде всего, не по действующему Статусу Роскомнадзора, утверждено постановлением Правительства Российской Федерации от 16 марта, 2009 г. № 2288, не содержащий регламентированного порядка государственного контроля в области обработки персональных данных, а также о проекте Положения о государственном контроле и надзоре за соответствием обработки персональных данных требованиям Федерального закона "О персональных данных"
В соответствии с пунктом 1 раздела I Положения о Роскомнадзоре от 16 марта 2009 года № 228 Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций осуществляет функции контроля и надзора за соблюдением персональных данных. обработка с

требованиями законодательства Российской Федерации в области персональных данных. Кроме того, Роскомнадзор является уполномоченным федеральным органом исполнительной власти по защите прав субъектов персональных данных.
Сегодня нормативная база, регулирующая распространение информации, обеспечивает конституционное право на защиту частной жизни и противодействует использованию информации, конфиденциальной информации в противоправных и преступных деяниях. При этом это не статичная система, а тенденция к развитию и совершенствованию материально-технической и нормативной базы.
Используемые информационные технологии участвуют в его создании, участвуют в его создании. Об этом свидетельствуют правила, разработанные другими странами, которые использовались при разработке законодательства в этой области.
Федеральный закон "Об информации, информатизации и защите информации" вводит понятие "персональных данных" (статья 2); увязывает персональные данные с конфиденциальной информацией и устанавливает, что перечни персональных данных должны устанавливаться федеральным законом (статья 11); Требует, чтобы деятельность неправительственных организаций и физических лиц по обработке и предоставлению персональных данных, а также по разработке, производству средств защиты информации и обработке персональных данных была лицензирована в порядке, установленном Правительством Российской Федерации.
Персональные данные определяются как любая информация, так или иначе связанная с конкретным лицом .
В соответствии с действующим законодательством состав персональных данных определяется оператором персональных данных в зависимости от целей их обработки. Как правило, операторов различных поставщиков услуг просят предоставить им контактные данные клиентов. Такие контактные базы поддерживаются не только для постоянных клиентов, но и для информации, получаемой в ходе рекламных кампаний. Вся эта информация является персональными данными.
Понятие «персональные данные» ранее было раскрыто в Указе Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня конфиденциальной информации» . Так, указ включает информацию о фактах, событиях и обстоятельствах личной жизни гражданина, позволяющую идентифицировать его личность (персональные данные), за исключением информации, которая должна распространяться в СМИ в случаях, установленных федеральными законами. в качестве конфиденциальной информации.
Статья 85 Трудового кодекса определяет персональные данные работника. Они включают информацию, необходимую работодателю в отношении трудовых отношений, связанных с конкретным работником.
Как упоминалось выше, персональные данные являются определенной информацией. В соответствии со ст. 2 ФЗ 27.07.2006 Н 149-ФЗ "Об информации, информационных технологиях и защите информации" информация является информацией (сообщениями, данными) самостоятельно. из формы презентации.
Информация может быть предметом публичных, гражданских и иных правоотношений, а также свободно использоваться любым лицом и передаваться от имени одного лица другому, если федеральными законами не установлены ограничения доступа к информации или иные требования к порядку ее распространения. предоставление или распространение. Поэтому информация классифицируется по категории доступа к ней по следующим типам
- информирование общественности;- информация, доступ к которой ограничен федеральными законами (информация ограниченного доступа) .
Таким образом, персональные данные граждан, за исключением общедоступных, являются информацией, доступ к которой ограничен законом.
Кроме того, вся информация в соответствии с Федеральным законом "Об информации, информационных технологиях и защите информации" делится на:
- свободно распространяемая информация;
- информация, предоставляемая по соглашению лиц, вовлеченных в соответствующие отношения;
- предоставление или распространение информации в соответствии с федеральными законами;
- Информация, ограниченная или запрещенная в Российской Федерации .
Существуют различные категории персональных данных, например:
- публичные персональные данные;
- специальные категории персональных данных;
- категории персональных данных, обрабатываемых в информационных системах персональных данных;
- биометрические персональные данные

Персональные данные может быть представлен как общая категория, включающая профессиональные и непрофессиональные (другие) секреты; Секрет личных данных является одним из видов секретов. Этот вывод следует из статьи 2 Закона «О персональных данных» , согласно которому его цель "заключается в обеспечении защиты прав и свобод человека и гражданина при обработке его персональных данных, включая защиту права на неприкосновенность частной жизни, личную и семейную тайну". Законодатель рассматривает действия по обработке персональных данных в режиме права на неприкосновенность частной жизни, личную и семейную тайну. Кроме того, в законе используется термин "конфиденциальность" в отношении личной информации, что в русском языке является синонимом "секретности". В силу ст. 7 настоящего закона конфиденциальность персональных данных не требуется: а) в случае обезличивания персональных данных; Б) в отношении общедоступных персональных данных. Таким образом, во всех остальных случаях (кроме указанных исключений) гарантируется конфиденциальность и есть основания говорить о режиме конфиденциальности персональных данных. Категория "конфиденциальность" носит более общий, оценочный характер. В западных странах на доктринальном уровне конфиденциальность часто понимается как свобода от любопытных глаз государства и отдельных лиц, как право человека на неприкосновенность частной жизни, анонимность и неприкосновенность частной жизни. Определение частной жизни включает право на личную неприкосновенность, независимость, достоинство и честь.
Частную жизнь можно определить как "жизнь человека в особой сфере семейных, бытовых, личных, интимных отношений, не подлежащих контролю со стороны государства, общественных организаций и граждан. Она включает в себя свободу частной жизни, размышлений, контактов с другими людьми, заявлений и юридических действий в области официальных отношений, тайны дома, дневники, другие личные дела, переписку, другую почту, тайну усыновления, гарантированную возможность доверить свои личные и семейные тайны священнику, врачу, адвокату, нотариусу, не опасаясь разглашения. А. Е. Лукашевич отметил: "Мы должны сосредоточиться на праве на личную и семейную жизнь и на сохранении ее тайн... Конфиденциальность можно определить как подконтрольную человеку физическую и духовную сферу, то есть свободную от внешнего воздействия. Законодательство не может вмешиваться в эту сферу, оно призвано защитить ее от любого незаконного вмешательства. "" Личная тайна "традиционно определяется как" часть информационного ресурса гражданина (физического лица), доступ к которому он определяет другим субъектам сам в рамках действующего законодательства ».
Таким образом, подсистема частной жизни включает список профессиональных секретов: юридических, медицинских, конфессиональных и т. д. В литературе обращается внимание на то, что все "профессиональные тайны" являются остатком тоталитарной оценки личного богатства, и имеют решающее значение для создания тайной личной жизни гражданина. Обязанность оставить его за специалистом следует считать вторичным, производным. Тайна присуща внутреннему миру человека, и её объём во многом зависит от богатства его внутреннего мира. Но особенности реализации права на неприкосновенность частной жизни связаны с тем, что определяется не предел реализации этого права, а граница вторжения в частную сферу посторонних лиц, в том числе работодателей. Мы считаем, что разумнее определить частную жизнь как сферу: "семья, домашнее хозяйство, взаимодействие, отношение к религии, внешняя деятельность, увлечения, досуг и т. д., которые человек не хочет обнародовать. В гражданском обществе реализация частных интересов и человеческих потребностей в рамках закона не подлежит контролю со стороны государства, любых организаций, в том числе тех, с которыми гражданин связан на службе.
Сведения о конфиденциальности, личной, семейной тайне могут быть переданы священнику, врачу, адвокату, нотариусу, не опасаясь их раскрытия, поскольку эти лица несут юридическую (врач, нотариус), корпоративную (адвокат) или религиозную (священник) ответственность .
Таким образом, под персональными данными понимается вся область человеческого поведения, реальная или потенциальная, не влияющая на общественные интересы, в которой люди имеют право самостоятельно, так или иначе, определять свой выбор действий. Термин "конфиденциальность" шире по охвату, чем термин "конфиденциальность", на который он ссылается. Последнее обычно относится к интимной сфере человеческих отношений. Конфиденциальность, помимо личной жизни, включает в себя выбор друзей, вкусы и предпочтения, увлечения и т. д.

3) На основании модели угроз ФСТЭК (5 февраля 21 года, скачать с сайта ФСТЭК), предположить нарушителей, их действия (техники и тактики).
Также в соответствии с этой моделью, предположить, какие действия осуществляет нарушитель в

отношении ИСПДН.
С развитием информационных технологий, которые незаменимо вошли во все сферы общественной жизни, параллельно начали развиваться технологии информационной безопасности (ИБ).
В настоящее время нормативная база в сфере защиты информации в РФ достаточно обширна: сюда входит защита государственных информационных систем, защита критической информационной инфраструктуры, защита персональных данных и т.д. Все эти требования обязывают практически каждое предприятие осуществляя деятельность в этих сферах, соблюдать требования по защите своих информационных ресурсов.
Согласно сложившейся практике и в соответствии с принятыми законодательными и нормативными документами, в целях обеспечения организационных и технических мер по защите информации ограниченного распространения специалисты по информационной безопасности выявляют угрозы безопасности информации (БИ), трансформируемой в сетях связи, информационных и телекоммуникационные инфраструктуры центров обработки данных и облачные инфраструктуры, информационные системы и автоматизированные системы управления (далее - объект информатизации).
Цель идентификации угроз достаточно проста – определить механизмы защиты информации объекта информатизации (ИО), и для достижения этой цели необходимо проанализировать всю доступную информацию об угрозах и уязвимостях. Для этого используются источники, содержащие информацию обо всех известных угрозах информационной безопасности, уязвимостях и описания векторов (схем) компьютерных атак. Эта информация содержится в таких базах данных, как База данных угроз информационной безопасности, реестрах, списках и классификациях CAPEC, ATT&CK, OWASP, STIX, WASC и т. д. Все это представляет собой общедоступные знания от экспертов по информационной безопасности.
В ходе изучения содержания этих источников любой специалист по информационной безопасности столкнется с массой трудностей, связанных с тем, как правильно применить весь объем накопленных знаний, изложенных в этих документах, к конкретному объекту информатизации и выявить актуальные угрозы информации.
В данной работе проведен анализу угроз нарушителей в области техники в отношении информационной безопасности в соответствии с опубликованным документом Федеральной службы по техническому и экспортному контролю - «Методика оценки угроз информационной безопасности» (утверждена ФСТЭК России 5 февраля 2021 г.). .
«Методика применяется для выявления угроз информационной безопасности, реализация (возникновение) которых возможна в системах и сетях, отнесенных к государственным и муниципальным информационным системам, информационным системам персональных данных, значимым объектам критической информационной инфраструктуры Российской Федерации, производственным информационные системы управления, используемые организациями военного назначения - промышленного комплекса, автоматизированные системы управления производственно-технологическими процессами на ответственных объектах, потенциально опасных объектах, сооружениях, представляющих повышенную опасность для жизни и здоровья человека и окружающей среды».
В основе данной методики лежит классический подход к оценке текущих угроз, а именно: выявление возможных рисков негативных последствий, которые возможны от реализации (возникновения) угроз информационной безопасности, выявление нарушителей как источника угроз, оценка возможностей нарушителя и формирование сценария реализации угрозы. На самом деле все логично: мы выявили риски, идентифицировали злоумышленника, определили его тактику и приемы (сформировали сценарий) и на основе этих данных приняли решение, актуальна угроза или нет.

4) Из банка данных угроз ФСТЭК (сайта) выбрать те угрозы, которые может реализовать актуальный нарушитель для защищаемой ИСПДН.
Ниже этот процесс более подробно рассмотрен на практике и отмечены трудности, которые могут возникнуть при учете всех критериев оценки угроз.
1. Обследование объекта информатизации
Документируется состав информационной системы (проводится инвентаризация компьютерного оборудования и сетей), в которую входят:
- описание сетей и систем (как объектов защиты) и их характеристик: назначение объекта информатизации; какие задачи (функции) он решает, состав обрабатываемой информации, защищена ли информация в соответствии с законодательством, основные процессы (бизнес-процессы), для которых создан пользовательский интерфейс;

- состав и архитектура ОИ: общесистемное программное обеспечение, прикладное программное обеспечение, программно-технические средства, используемые средства защиты информации;
- подключение к сетям телекоммуникаций: Интернет, информационным и телекоммуникационным сетям других организаций;
- технологии, используемые в ОИ: съемные носители, технологии виртуализации, технологии беспроводного доступа, мобильное оборудование, веб-серверы, технологии удаленного доступа, электронная почта и т.д.

2. Определение вероятных негативных последствий реализации (возникновения) BI-угроз.

В ходе исследования и выявления актуальных угроз информационной безопасности определяются разрушительные последствия, которые могут наступить при реализации (возникновении) угроз BI. Деструктивные последствия выявляются в связи с нарушением основных процессов, реализацию которых обеспечивает ОР.

На основе определенных негативных последствий формируются риски (ущерб). Методика предлагает рассматривать типичные виды рисков (ущерба) по трем направлениям:
- ущерб, который может понести субъект;
- опасности, угрожающие юридическому лицу или индивидуальному предпринимателю, связанные с производственно-хозяйственной деятельностью;
- ущерб, угрожающий стране в сфере обеспечения обороноспособности государства, государственной безопасности и внутреннего правопорядка, а также в других сферах деятельности.

Основная сложность заключается в том, что методология не содержит инструментов, с помощью которых можно было бы определить негативные последствия конкретного риска (ущерба), применимого к системе. Здесь оператор системы полагается исключительно на собственные методики: например, согласно 152-ФЗ, при обработке персональных данных оператор должен оценить вред, который может быть причинен субъектам персональных данных (п. 5 ст. 18.1). Также для объектов критической информационной инфраструктуры согласно Постановлению Правительства № 127 от 2018 года определен перечень показателей критериев значимости, на основании которых определяются последствия для системы.

Пример: информационная система автоматизирует процесс формирования графика приема врача для электронного регистратуры. При нарушении этого процесса негативными последствиями будут невозможность (прерывание) оказания медицинской помощи, а риск будет выражаться в нанесении ущерба личности, а возможно даже жизни и здоровью, поскольку заболевание может быть не диагностировано вовремя. , и т. д.

3. Возможные объекты угроз информационной безопасности.

«При оценке угроз информационной безопасности, информационным ресурсам и компонентам объекта информатизации несанкционированный доступ к которому или воздействие на который в ходе реализации (возникновения) угроз информационной безопасности может привести к негативным последствиям».

На основе анализа полученных данных и данных обследования систем и сетей определяются направления использования информационных ресурсов и интегрированных систем и сетей, которые с высокой степенью вероятности могут быть объектами воздействия. Объекты воздействия должны быть идентифицированы на аппаратном, системном и прикладном уровнях, на уровне модели сетевого взаимодействия, а также на уровне пользователя. Для каждого объекта воздействия определены виды воздействия на него, которые могут привести к негативным последствиям.

Пример: объект воздействия – автоматизированные рабочие места пользователей; негативные последствия – нарушение конфиденциальности (утечка) персональных данных; виды воздействия - нарушение функционирования (работоспособности) программных и технических средств автоматизированного рабочего места.

4. Источники угроз информационной безопасности

Потенциальными источниками угроз могут быть человеческий фактор, техногенные или естественные носители угроз безопасности.

Для ОИ важно выявить возможные антропогенные источники угроз информационной безопасности, к которым могут относиться субъекты (группа лиц), представляющие угрозу информационной безопасности посредством несанкционированного доступа и (или) воздействия на информационные ресурсы и (или) компоненты информационный объект.

Антропогенный источник угроз – нарушитель информационной безопасности, которым может быть физическое лицо, случайно или умышленно совершившее действия, приводящие к нарушению безопасности информации при ее обработке в информационных системах техническими средствами.

Есть внутренние и внешние нарушители. Инсайдер — злоумышленник, находящийся внутри информационной системы в начале процесса реализации угрозы. Внешний злоумышленник – злоумышленник, находящийся вне информационной системы в начале процесса реализации угрозы.
Для успешной реализации угроз в IP внешний злоумышленник должен определенным образом получить доступ к процессам, запущенным в информационной системе. В этом случае внешний злоумышленник должен совершать все свои дальнейшие действия под именем созданной им новой сущности или той, которая ранее существовала в системе.
К внутренним нарушителям, согласно ГОСТ 53113.1-2008, относятся инсайдеры. В то же время они могут следовать инструкциям субъектов, находящихся за пределами информационной системы.
Для каждого типа нарушителей формируется цель реализации угроз информационной безопасности и на основе этой цели делаются предположения о классификации возможных нарушителей.
Пример: объект информатизации – медицинская информационная система коммерческой лечебно-профилактической организации. Тип нарушителя – спецслужбы иностранных государств; возможные цели нарушителя – причинение ущерба государству в сфере обороны, безопасности и правопорядка; предположения о отнесении к возможным злоумышленникам – цели не предполагают потенциального присутствия злоумышленника, поскольку медицинская информационная система не может нанести никакого ущерба государству в сфере обороны. Тип нарушителя – физические лица (злоумышленники); возможные цели нарушителя – получение выгоды (финансовой или материальной); предположения о том, что они отнесены к возможным злоумышленникам – возможные объекты угроз информационной безопасности предполагают наличие злоумышленника, поскольку хакер может шифровать данные и осуществлять финансовый шантаж.
Далее производится сравнение возможных нарушителей и их целей реализации BI-угроз с вероятными негативными последствиями и видами рисков (ущерба) от реализации (возникновения) BI-угроз. По результатам сравнения фактические нарушители определяются по следующему принципу: «нарушитель считается актуальным, если возможные цели реализации нарушителем угроз информационной безопасности могут привести к определенным негативным последствиям для информационной безопасности и соответствующим рискам (виды ущерба)».
Пример: тип нарушителя – физические лица (злоумышленники); цели правонарушителя – получение выгоды (финансовой или материальной); вид риска (ущерба) состоит в причинении ущерба физическому лицу (финансовый, иной материальный ущерб физическому лицу, нарушение конфиденциальности (утечка), частной жизни). Персональная информация). Из этого примера видно, что хакер, создавая угрозу информационной безопасности, может нанести ущерб физическому лицу или его персональным данным, обрабатываемым на объекте информационных технологий.
Результатом действий, предпринятых в соответствии с настоящим пунктом, является список правомочных нарушителей BI и уровня их возможностей. Уровень способности конкретного нарушителя реализовывать BI-угрозы можно определить с помощью таблицы 9.1 «Методы оценки угроз информационной безопасности».
5. Способы реализации (возникновения) угроз информационной безопасности.
В процессе оценки угроз BI должны быть определены наиболее вероятные способы реализации угроз информационной безопасности, посредством использования которых соответствующие нарушители в данном случае могут реализовать угрозы BI на объекте информационных технологий.
Процесс определения наиболее вероятных способов реализации (возникших) угроз безопасности включает в себя составление перечня рассматриваемых (возможных) способов реализации угроз безопасности.
Основными способами реализации (возникновения) угроз информационной безопасности могут быть: уязвимости программного обеспечения, вредоносное ПО, использование необъявленных функций программного обеспечения, закладки (программные и аппаратные), атаки, ошибочные действия и т.п.
Необходимо определить границы между объектами воздействия, которые определяются на основе изучения и анализа данных, полученных при обследовании загрязняющих веществ:
- об архитектуре, составе и условиях работы операционной системы;
- о группах пользователей IP, их типах доступа и уровнях полномочий.
Результатом процесса определения реальных способов реализации (возникновения) угроз BI является описание способов реализации (возникновения) угроз информационной безопасности, которые могут быть использованы реальными злоумышленниками, и описание интерфейсов объектов воздействия. доступны для использования реальными нарушителями.
Пример: тип правонарушителя – отдельные лица (хакеры); категория правонарушителя – внешний; объекты

воздействия – сетевой трафик; доступные интерфейсы – каналы связи с внешними информационными и телекоммуникационными сетями; методы реализации – эксплуатация уязвимостей в сетевых конфигурациях, ошибочные действия в процессе создания и использования систем и сетей, в том числе при установке, настройке аппаратного и программного обеспечения, перехвате сетевого трафика передачи данных, проведении DoS-атак.

6. Текущие угрозы BI

В ходе анализа и оценки угроз информационной безопасности определяются вероятные угрозы информационной безопасности и оценивается их соответствие объекту информатизации - актуальные угрозы информационной безопасности.

В качестве исходного перечня угроз информационной безопасности необходимо использовать базу данных угроз информационной безопасности, сформированную ФСТЭК России (http://bdu.fstec.ru/) .

База данных угроз информационной безопасности содержит информацию об основных угрозах информационной безопасности и уязвимостях, характерных в первую очередь для государственных информационных систем и автоматизированных систем управления производственными и технологическими процессами ответственных объектов.

База данных угроз информационной безопасности не имеет иерархической структуры; Если загрузить информацию об угрозах в виде электронной таблицы, то доступна сортировка по источникам угроз (нарушителям), объектам воздействия и последствиям. Фактически мы можем изначально устранить угрозы, неприменимые к нашему объекту информатизации.

Пример: Информационная система не использует платформы виртуализации и оборудование виртуальной инфраструктуры, то есть отсутствуют объекты воздействия, такие как виртуальная машина или гипервизор; соответственно, угрозы, применимые к этим объектам, должны быть исключены из перечня соображений.

Далее процесс выбора возможных угроз из оставшегося списка угроз безопасности информации баз данных осуществляется по следующему принципу: угроза BI признается возможной при наличии злоумышленника или иного источника угрозы, объекта влияние, способ реализации угрозы информационной безопасности, а также реализация угрозы может привести к негативным последствиям.

«Выглядит это так: УБД = [нарушитель (источник угрозы); объекты воздействия; способы реализации угрозы; негативные последствия]».

Пример: UBI — угроза аппаратного сброса пароля BIOS (UBI.004); источником угрозы является внутренний злоумышленник с базовыми возможностями, внутренний злоумышленник с базовыми расширенными возможностями; цель — BIOS/UEFI; способами реализации угрозы являются несанкционированный физический доступ и (или) воздействие на технические средства, компьютерные носители; негативные последствия – необходимость дополнительных (внеплановых) затрат на приобретение товаров, выполнение работ или оказание услуг (в том числе приобретение программного обеспечения, вышедшего из строя оборудования, замену, настройку, ремонт этих предметов).

Из сформированного списка возможных угроз информационной системе необходимо оценить возможные угрозы на актуальность. Указанные мероприятия осуществляются по следующему принципу: угроза признается актуальной при наличии хотя бы одного сценария реализации угрозы информационной безопасности.

5) Используя приказ ФСТЭК №21(с его обновлениями), подобрать меры по защите ИСПДН от выбранных актуальных угроз.

Приказ ФСТЭК 21 найдете на сайте , в него вступали некоторые обновления, прочитайте все документы по обновлению приказа ФСТЭК № 21, начиная с 2012 года (тоже на сайте ФСТЭК). Меры подбираются в соответствии с раннее установленным уровнем защищенности ИСПДН. Для выбора мер можно использовать сайт ФСТЭК (БАНК МЕР ФСТЭК).

«Определение сценариев включает в себя установление последовательности возможных тактик и соответствующих приемов, которые может использовать реальный злоумышленник с соответствующим уровнем возможностей, а также наличие интерфейсов для использования соответствующих методов реализации угроз информационной безопасности. Несмотря на то, что методология предоставляет перечень основных тактик и соответствующие стандартные приемы, она может быть дополнена при построении сценариев реализации угроз информационной безопасности» .

Пример международной угрозы: UBI; - Угроза аппаратного сброса настроек биоса (UBI.004); источником угрозы является внутренний злоумышленник с базовыми возможностями, внутренний злоумышленник с

базовыми расширенными возможностями; объект воздействия – BIOS/UEFI; способы угрозы представляют собой несанкционированный физический доступ и (или) воздействие на технические средства, компьютерные носители; негативные последствия - необходимость дополнительных (внеплановых) затрат на приобретение товаров, работ или услуг (в том числе приобретение программного обеспечения, оборудования, вышедшего из строя, замену, замену, ремонт этих средств). Сценарии реализации угрозы – использование тактики 1: сбор информации о телекоммуникациях и сетях (тактическая задача: злоумышленник стремится получить любую техническую информацию, которая может быть полезна при реализации угрозы информационной безопасности); метод: сбор информации о пользователях, устройствах, приложениях путем поиска информации в памяти, файлах, каталогах, базах данных, прошивках устройств, хранилищах исходного кода программного обеспечения, в том числе поиск паролей в исходном и хешированном виде, криптографических ключей; применение тактики 2: получение первоначального доступа к компонентам системы и сети; Аппаратное обеспечение: несанкционированный доступ с использованием учетных данных сотрудника или законного пользователя (методы перебора, атаки по словарю, пароли по умолчанию производителя, использование одних и тех же паролей для разных учетных записей, использование таблиц Rainbow и т. д.).

Проблема заключается в том, что все содержащиеся в ней угрозы представляют собой единичные действия. В реальности этого не происходит: чтобы сделать что-то плохое с информационной системой, сначала нужно проделать большую подготовительную работу: получить доступ к нужному сегменту инфраструктуры (или хотя бы к некоторым, если доступа к инфраструктуре вообще нет), загрузить инструменты, собрать информацию о системе, находить уязвимые узлы, получать контроль над ними и т.д. поэтому любая более или менее сложная атака превращается в тактическую игру, где в каждый ход нарушитель решает определенную тактическую задачу и планирует следующий ход, исходя из того, что он получил в результате текущего хода. Ребята из MITRE определили двенадцать тактических задач (tactics), которые должен решить нарушитель и из которых формируется сценарий его "игры"

Первоначальный доступ: "первичное проникновение", возможность каким-либо образом добраться до элементов атакуемой инфраструктуры. Методы ("techniques" в терминах Att&CK) могут быть разными, от использования общедоступного уязвимого внешнего интерфейса до социальной инженерии и подключения к инфраструктуре ваших собственных устройств.

Выполнение: возможность каким-либо образом заставить атакуемый элемент инфраструктуры выполнить хотя бы некоторые действия, необходимые нарушителю. Методы, опять же, могут быть самыми разными, от использования готового интерфейса командной строки до заражения узла вредоносным ПО.

Постоянство: способность сохранять присутствие в атакованной инфраструктуре даже после перезагрузки атакованного узла, обнаружения и уничтожения некоторых встроенных инструментов и других методов... - Ну, вы поняли.

Повышение привилегий: если казнь - это выполнение хотя бы каких-то действий, то здесь нарушитель пытается "получить" недостающие возможности.

Уклонение от защиты: противодействие противодействию. Жертва может использовать различные приемы для обнаружения и блокирования действий преступника, а он пытается их обойти.

Доступ к учетным данным, на самом деле, является одной из ключевых тактик, она включает в себя различные способы перехвата, восстановления, выбора или повторного использования паролей, ключей, токенов аутентификации и т.д. Если нарушителю удается получить контроль хотя бы над каким-то узлом инфраструктуры, эта тактика всегда заканчивается получением учетной записи администратора предприятия - таковы суровые реалии современной информационной безопасности.

Обнаружение: сбор любой возможной информации, которая может оказаться полезной для успешного запуска или разработки атаки. Это включает анализ общедоступной информации с помощью инструментов OSINT и вдумчивое изучение "внутренностей" успешно атакованных элементов инфраструктуры.

Боковое перемещение: "расползание" по атакованной инфраструктуре, расширение своего присутствия. "Хватайте все, до чего сможете дотянуться, - тогда мы посмотрим, как это использовать". Согласно используемым техникам, это то же самое, что и первоначальный доступ, но только после успешного преодоления периметра, когда появляется гораздо больше возможностей "захватить" элементы внутренней инфраструктуры.

Командование и контроль - задача, связанная с постоянством: обеспечить удаленное управление контролируемыми узлами инфраструктуры, а в некоторых случаях и возможность "работать руками" на узле, к которому злоумышленник не должен иметь удаленного доступа.

Сбор, эксфильтрация, воздействие, последние штрихи успешной атаки: сбор информации, представляющей

интерес для злоумышленника (и выгрузка ее наружу, что, учитывая ее объем, может оказаться совершенно нетривиальной задачей), а также все возможные деструктивные действия.
На тактическом уровне любую сколь угодно сложную атаку можно описать языком, понятным неспециалисту: они получили доступ к веб-интерфейсу системы, благодаря кривой конфигурации Apache и уязвимостям ядра ОС смогли получить контроль над ОС, перехватили трафик, в котором передавался пароль администратора незашифрованный, ... Но это легко сделать только для конкретного сценария, но при моделировании угроз вы должны учитывать множество возможных вариантов.
Каждой тактике соответствует определенное количество приемов – известных приемов, которые позволяют правонарушителю выполнить необходимое действие в рамках решения тактической задачи, стоящей перед ним в данный момент. Итак, если информационная система имеет общедоступный веб-интерфейс (даже если публично доступна только страница авторизации), то у нарушителя есть целый набор возможностей, каждая из которых потенциально может предоставить ему, пусть и ограниченный, доступ к этой сети.
В какой-то момент в приложении может появиться уязвимость, которая позволит злоумышленнику внедрить в CMS собственный модуль;
В какой-то момент в приложении может появиться уязвимость, позволяющая злоумышленнику выполнить команду операционной системы, SQL-запрос или собственный скрипт;
В какой-то момент в приложении может быть обнаружена уязвимость, которая позволит злоумышленнику выполнить собственный скрипт в браузере пользователя;
В какой-то момент в приложении может быть обнаружена уязвимость, которая позволит злоумышленнику загрузить конфиденциальную информацию, например, хэши паролей пользователей или, не дай Бог, сами пароли в открытом виде;
В какой-то момент в приложении может появиться учетная запись пользователя со словарным паролем (или паролем, успешно полученным в результате атаки на другой элемент инфраструктуры) и т.п.
Поскольку мы не фантазируем при моделировании угроз, а ограничиваемся внешними методами атак, то для каждого элемента инфраструктуры, в зависимости от его роли, существует определенный перечень применимых к нему методов: существует набор методов атак на веб-интерфейсы. , в беспроводных сетях, сетевой инфраструктуре, в домене MS AD, на рабочих местах с использованием социальной инженерии и без нее и т. д. В понятие «технология» входят:
Данная технология подходит для определенного класса уязвимостей, которые могут присутствовать в информационной системе «с рождения» или появляться в процессе эксплуатации. Причем формулировка «может появиться» — это скорее дань политкорректности: вероятность появления таких уязвимостей напрямую зависит от уровня безразличия, присущего ИТ-отрасли на всех этапах жизненного цикла информационной системы, и сейчас это было бы честнее сказать: «они неизбежно рано или поздно появятся». "
Определенные приемы, используемые преступником. То есть, когда мы говорим «STP позволяет перенаправлять и перехватывать трафик», мы говорим не о теоретической возможности, а о четко определенной последовательности действий, которую можно продемонстрировать.
Определенные последствия, включая приобретение правонарушителем определенных способностей. Опять же, когда мы говорим «доступность протокола STP для армий пользователей плохая», это означает вполне конкретные последствия: злоумышленник может перехватывать трафик (и это дает ему возможность использовать «пассивные» методы, основанные на анализе трафика) или , при неосторожном использовании "выбрасывает" ядро из сети.
Определенные следы, которые оставляет применение этой техники и по которым можно обнаружить ее применение – во время нападения или в ретроспективе. Именно поэтому в нормативных документах ФСБ обнаружением атак называют не использование идентификаторов, а комплекс действий по анализу различных событий, привязывая их к определенным методикам.
Определенные «целевые» контрмеры. Не абстрактные «установить SIEM», «проанализировать программный код», «управлять конфигурацией», а «настроить такие корреляции», «сделать так, чтобы такие конструкции не появлялись в коде» и «похлопать админа по запястью». при попытке изменить эти параметры».
При моделировании угроз на техническом уровне становится возможным оценить достаточность используемых мер защиты уже на этапе разработки технического задания.
Таким образом, процесс рассмотрения угроз информационной безопасности и отнесения их к актуальным достаточно трудоемкий, а для качественной оценки методика требует участия экспертной группы, в которую входят специалисты по информационной безопасности, специалисты по информационным

технологиям и т.д. Это общепринято что не каждый оператор имеет квалифицированный персонал, способный проводить такие оценки, даже если в штате есть один специалист, такие меры могут привести к занижению прогнозов и предположений при угрозе риска или, наоборот, к завышению, что может привести к непредвиденным последствиям. ущерб (риски) или неоправданные затраты на нейтрализацию (блокировку) угроз, не имеющих отношения к действию.

6) В соответствии с установленными мерами подобрать средства защиты ИСПДН.
Российская Федерация как высокоразвитая страна, использующая большинство информационных технологий, в условиях глобализации современного мира не может не использовать нормативные правовые акты, защищающие системы современного мира. С этой целью Российская Федерация создает нормативную базу, состоящую из действующего законодательства Российской Федерации.
Несмотря на то, что эта система де-юре показывает, что эта система не завершена. Существует неясность в положениях Закона, которые по-разному толкуются государственными регуляторами и операторами.
В текущей экономической ситуации у нас ограниченный ресурс уполномоченных органов по защите данных, что не позволяет выполнять надзорные функции в полном объеме.
Персональные данные, как неотъемлемая часть информации, защищены в любом режиме ограничения доступа, а иногда персональные данные просто составляют тайну, например, медицинскую, банковскую, страховую тайну.
Система обеспечения конфиденциальности персональных данных регулируется Федеральным законом "О персональных данных", Постановлением Правительства № 1119 и рекомендациями ФСТЭК России. Закон описывает основные термины и определения, устанавливает права и обязанности оператора, в том числе в области выбора средств защиты персональных данных, и ответственность операторов. Постановление Правительства определяет критерии, по которым информационные системы персональных данных относятся к разным уровням безопасности. Приказ ФСТЭК России № В 21 названы конкретные 15 групп технических мер, используемых для обеспечения безопасности. В каждой группе также определены средства, которые оператор имеет право использовать.
Классификация систем защиты персональных данных
Информационные системы персональных данных делятся по уровням безопасности – от низкого до максимального. Этот рейтинг зависит от количества людей, чьи данные обрабатываются, и от характеристик данных. В соответствии с рейтингами системы защиты данных делятся операторами на две группы:
-типичный;
-особенные.
К первой группе относятся системы, задачей которых является только обеспечение конфиденциальности и сохранности данных. Концепция конфиденциальности подразумевает соблюдение двух параметров:
-обработка данных разрешена только лицам, специально уполномоченным на это внутренней документацией организации-оператора;
Данные передаются только в том случае, если они зашифрованы.
Для специальных систем защиты данных, в дополнение к характеристике конфиденциальности, требуется обеспечить дополнительные меры защиты, по крайней мере, одну из перечисленных. К ним относятся:
-целостность. Этот термин подразумевает, что любые изменения в данные вносятся только регламентированным образом, например, только лечащий врач имеет право вносить изменения в амбулаторную карту пациента. Также целостность обеспечивается передачей данных по телекоммуникационным сетям только с использованием электронной подписи;
-доступность. Концепция предполагает, что система используется только определенными пользователями и в течение определенного периода времени.
Существуют две группы специальных систем, которые требуют использования специальных средств защиты данных:
-обработка данных, связанных со здоровьем человека;
-обработка персональных данных таким образом, чтобы результат работы становился основой для принятия юридически значимых решений.
Также системы защиты конфиденциальных данных можно разделить на автономные, не имеющие прямого подключения к телекоммуникационным сетям, и имеющие такие подключения, которые требуют повышенной тщательности для обеспечения безопасности информации.

Выбор технических средств защиты персональных данных

Выбор средств автоматизации, используемых для обеспечения безопасности при обработке персональных данных, в конечном счете зависит от таких параметров:

-уровень безопасности информационной системы персональных данных, требуемый Постановлением Правительства;

-финансовые и организационные возможности операторов;

-технические решения, используемые для обеспечения безопасности;

-наличие или отсутствие лицензии ФСТЭК.

Основываясь на этих параметрах, оператор может добавить упреждающие меры к основным средствам защиты персональных данных, чтобы система достигла уровня безопасности, соответствующего текущим угрозам субъектам персональных данных и их информационным правам.

Таким образом, оператору необходимо обеспечить доступность технических средств, способных:

-идентифицировать и аутентифицировать пользователей, устанавливать индивидуальные уровни доступа к определенным категориям персональных данных;

-контролировать вывод данных из системы, например, передачу по почте или мессенджеру, перенос на съемные носители. Системы DLP и SIEM могут решить эту проблему. Кроме того, необходимо обеспечить шифрование информации, передаваемой по обычным каналам связи или находящейся непосредственно в информационных базах данных, с использованием средств криптографической защиты;

-обеспечить максимально возможную защиту информационных баз персональных данных, подключенных к телекоммуникационным сетям, от внешних атак. Для этого требуется установка антивирусной защиты, других методов защиты от хакерских и иных атак, использование электронной подписи, шифрование исходящего трафика с использованием ключей и сертификатов, сгенерированных пользователем и зарегистрированных в центрах сертификации;

-регистрировать все действия пользователя в системе, что повышает уровень как безопасности персональных данных, так и мотивации сотрудников к ее обеспечению.

Технические средства и программные продукты должны быть сертифицированы ФСТЭК России по классу не ниже АК2 по классификации ФСБ РФ. Например, операционной системой, соответствующей этому классу, является Windows XP с пакетом обновления Secure Pack Rus. Специальные системы требуют соответствия всем требованиям данного класса безопасности. Дополнительно потребуется сертификация ФСТЭК Российской Федерации помещений, в которых расположены компьютеры. Раз в три года необходимо проверять соответствие используемых средств действующим требованиям.

Содержание понятия "конфиденциальная информация" в наименовании лицензируемой деятельности определяется Федеральным законом "О лицензируемой деятельности" (пункты 10 и 11 части 1 статьи 17), и содержание лицензируемой деятельности (пункт 11) требует уточнения.

Уведомление об использовании персональных данных: оператор обязан уведомить уполномоченный орган по защите прав субъектов данных о намерении обрабатывать персональные данные.

Оператор имеет право обрабатывать персональные данные, относящиеся к уполномоченным данным, имеющим трудовые отношения с оператором без уполномоченного органа по защите прав субъектов данных.

Противоречия между законом и постановлением правительства. Требование о потенциальном операторе конфиденциальной информации во всех случаях, включая те, где используется обработка конфиденциальных данных (например, в рамках трудовых отношений), не следует из Федерального закона "О персональных данных" и в широком смысле.

Противоречия между законом и постановлением правительства.

1. Классификация информационных систем системы данных "по объему обрабатываемых ими данных и угрозе для жизненно важных лиц, общества и государства".

2. Требование к операторам связи обеспечивает защиту каналов связи, по которым осуществляется обмен персональными данными.

Противоречия между законом и нормативным актом ведомств.

1. Отделение персональных данных, идентифицирующих пользователей данных, от общего объема персональных данных,

2. Отделить задачу защиты конфиденциальной информации от задач защиты конфиденциальной информации.

Кроме того, правительство не использует бюджетные средства для обеспечения своей безопасности (включая лицензирование и сертификацию систем защиты информации для систем обработки

конфиденциальной информации, а также средств массовой информации такой информации).
Услуги специалистов не предоставляются в школах, детских садах, поликлиниках, соответственно, отсутствуют элементарные помещения, отвечающие техническим стандартам и требованиям к технической информации .
Соблюдение всех необоснованных требований к предприятию, будь то приобретение необходимого технического оборудования, создание специальных помещений, обучение персонала, изготовление электронных ключей, влечет за собой значительные материальные затраты, а механизмы финансирования со стороны государства для них не предусмотрены.
Частота и масштабы незаконного сбора и обработки данных не уменьшились, и государство практически не контролирует этот процесс.
Несмотря на то что операторы передачи данных готовы соблюдать закон, они не до конца понимают, как это сделать. В большинстве случаев доступ к персональным данным не контролируется, а утечка информации не отслеживается. Во многих случаях данные передаются между кампаниями по открытому каналу без предварительного шифрования. Доступ к базам данных предоставляется довольно большому числу людей, не имеющих никакого отношения к сбору, хранению и представлению данных.
Законодательное регулирование защиты данных до сих пор не работает, а федеральный закон "О закрытых данных" по-прежнему выдвигает только общие и неспецифические требования. Каждая кампания интерпретирует эти требования по своему усмотрению, а иногда просто игнорирует их .
При этом нет единого органа, который следил бы за сбором и оказывал бы специализированные услуги. Обмен персональными данными осуществляется по открытому каналу. Он основан на информационном программном обеспечении, разработанном в других странах.
На данный момент в РФ не хватает специалистов в области криптологии (шифрования данных). При этом наблюдается лавина электронных сервисов с использованием персональных данных (развитие социальных сетей, электронный документооборот, создание электронных архивов в медицине, развитие интернет-торговли, электронной переписки, появление электронных денег и т. д.).
В современных условиях появляется все больше клиентских баз, что приводит к показателям коррупции в этой сфере и недобросовестной конкуренции . Утечка информации из медицинских учреждений и СМИ приводит к моральному приему.
Не всегда соблюдаются требования Закона о персональных данных. Хранение персональной информации должно осуществляться не дольше, чем требуется для ее обработки, а при достижении целей обработки или при необходимости их персональная информация должна быть уничтожена. Срок, в течение которого устанавливаются ненужные персональные данные, должен быть уничтожен, установленный в три рабочих дня (ч. 2 ст. 5 ФЗ № 152 "О персональных данных") . Например, в медицинских учреждениях персональные данные могут храниться годами.
При обработке персональных данных оператор обязан принять необходимые организационно-технические меры, в том числе с использованием шифровальных (криптографических) средств, для защиты ценностей персонализированных данных, копирования, распространения персональных данных, а также от иных противоправных действий. Как только эти требования не могут быть выполнены на месте, поскольку нет специальных помещений, защищенных компьютерных внутренних сетей, криптографических программ и подходящего обучения. Использование и хранение биометрических персональных данных вне информационных систем персональных данных, возможность реализации только на таких материальных носителях используется с использованием такой технологии защиты от применения технологии защиты. уничтожение, модификация, блокировка, копирование и распространение. На самом деле, мой тип - отсутствие специальных серверов, которые хранят персональные данные, защищенные сети связи с этими серверами, свободный доступ к оборудованию, Еще одно слабое звено в области защиты персональных данных - недостаточная правая подготовка как лиц, работающих в области сбора и хранения персональных данных, таких и обычных.
Недостаточное финансирование на укрепление материально-технической базы в сфере защиты персональных данных играет очень важную роль в современной экономической ситуации в мире. В частности, сегодня банки обрабатывают огромный объем персональных данных, к которым имеет доступ ряд корпоративных департаментов и ведомств. В большинстве случаев этот доступ не контролируется, что приводит к высоким рискам утечки . С учетом актуальности проблемы следует признать, что защита персональных данных граждан является неотъемлемой частью гарантии защиты права и свободы граждан в демократическом обществе. Законодательство в этой области, устранение противоречий между нормативными правовыми актами и материально-техническим обеспечением).

Нужно создать:
- единый орган, контролирующий безопасность деятельности; - установить связи между организациями, использующими персональные данные, и хранителями закрытых электронных сетей;
- обеспечить профессиональную подготовку, персонализированные методы защиты и защиты.
- необходимо обеспечить предоставление доступа к личным данным. только по решению суда.
- разработка программ электронного шифрования данных.
Необходимо, чтобы программа электронного и шифрования данных, операционные системы разрабатывались отечественными специалистами для предотвращения намеренного взлома программы, обеспечивая возможности контроля - предоставить материальные ресурсы, современное оборудование и квалифицированных специалистов организации, занимающейся сбором, хранением и передачей персональных данных; - на законодательном уровне доработать меру ответственности не только для юридических лиц, но и для физических лиц, которые собирают, хранят и передают персональные данные.
В настоящее время существуют различные органы осуществляющие надзор за деятельность в области защиты персональных данных. Главным из них является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Основными полномочиями государства в области защиты персональных данных является нормативное регулирование, а так же установление конкретных полномочий органов государственной власти и операторов в области обработки персональных данных. К полномочиям органов государственной власти так же относится разработка доктрины информационной безопасности в области персональных данных и разработка механизма защиты в случае незаконного распространения персональных данных.
В ходе реализации положений законодательства о защите персональных данных можно отметить проблемы реализации государственных полномочий в указанной области.
Среди основных проблем можно отметить отсутствие единой системы государственных органов в области защиты персональных данных, отсутствие эффективного взаимодействия между органами, осуществляющими использование персональных данных, распространённость безосновательного предоставления доступа к персональным данным, отсутствие шифрования персональных данных при передаче.
Устранение указанных проблем поможет повысить эффективность государственного управления в области защиты персональных данных.

Заключение

В завершении исследования можно прийти к следующим выводам. Под персональными данными понимается любая информация о физическом лице, неправомерное распространение которой может привести к возникновению ущерба и нарушении конституционных прав гражданина. Защита персональных данных осуществляется на законодательном уровне. Любой гражданин вправе ограничить и запретить доступ к своим персональным данным. В случае нарушение права на защиту персональных данных граждане вправе обратиться к уполномоченным органам либо в суд с требованиям об устранении нарушения права на защиту персональных данных, а так же праве требовать материального возмещения причиненных убытков.

В настоящее время существуют различные органы осуществляющие надзор за деятельность в области защиты персональных данных. Главным из них является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Основными полномочиями государства в области защиты персональных данных является нормативное регулирование, а так же установление конкретных полномочий органов государственной власти и операторов в области обработки персональных данных. К полномочиям органов государственной власти так же относится разработка доктрины информационной безопасности в области персональных данных и разработка механизма защиты в случае незаконного распространения персональных данных.

В ходе реализации положений законодательства о защите персональных данных можно отметить проблемы реализации государственных полномочий в указанной области.

Среди основных проблем можно отметить отсутствие единой системы государственных органов в области защиты персональных данных, отсутствие эффективного взаимодействия между органами, осуществляющими использование персональных данных, распространённость безосновательного предоставления доступа к персональным данным, отсутствие шифрования персональных данных при передаче.

Процесс рассмотрения угроз информационной безопасности и отнесения их к актуальным достаточно трудоемкий, а для качественной оценки методика требует участия экспертной группы, в которую входят специалисты по информационной безопасности, специалисты по информационным технологиям и т.д. Это общепринято что не каждый оператор имеет квалифицированный персонал, способный проводить такие оценки, даже если в штате есть один специалист, такие меры могут привести к занижению прогнозов и предположений при угрозе риска или, наоборот, к завышению, что может привести к непредвиденным последствиям. ущерб (риски) или неоправданные затраты на нейтрализацию (блокировку) угроз, не имеющих отношения к действию.

Список использованной литературы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) // Российская газета. 2020. N 144
2. Международная конвенция «Об охране личности в отношении автоматизированной обработки персональных данных» 1981 г.[Электронный ресурс] режим доступа http://www.consultant.ru/document/cons_doc_LAW_121499/ (дата обращения 20.12.2023)
3. Европейская конвенция о защите физических лиц при автоматизированной обработке персональных данных // Собрание законодательства РФ. 2014. N 5.
4. Конвенция о защите физических лиц при автоматизированной обработке персональных данных" (Заключена в г. Страсбурге 28.01.1981) (вместе с Поправками к Конвенции о защите физических лиц при

автоматизированной обработке персональных данных (СДСЕ № 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15.06.1999) // Собрание законодательства РФ. 2014. № 5. Ст. 419.
5. Директива 97/66 / ЕС от 15 декабря 1997 г. по обработке персональных данных и защите конфиденциальности в телекоммуникационном секторе. .[Электронный ресурс] режим доступа https://base.garant.ru/2570354/ (дата обращения 20.12.2023)
6. Налоговый кодекс Российской Федерации (часть первая)" от 31.07.1998 № 146-ФЗ (ред. от 19.12.2023)// Собрание законодательства РФ.-1998.- Ст. 3824.
7. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 12.12.2023) «Об информации, информационных технологиях и о защите информации» //Собрание законодательства РФ.2006. N 31 (1 ч.), Ст. 3448.
8. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 12.12.2023) «Об информации, информационных технологиях и о защите информации» //Собрание законодательства РФ.2006. N 31 (1 ч.), Ст. 3448.
9. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 06.02.2023) «О персональных данных»// Собрание законодательства РФ.-2006. -№ 31- (1 ч.).-Ст. 3451.
10. Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О противодействии терроризму и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» № 374-ФЗ // Собрании законодательства РФ. 2016. № 28 Ст. 4558.
11. Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня конфиденциальной информации» (ред. от 13.07.2015) // Собрание законодательства РФ -1997.-№ 10.- Ст.-1127.
12. Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»// Собрании законодательства РФ. 2016. N 50 Ст. 7074.
13. Методический документ «Методика оценки угроз безопасности информации» (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.). - 83 с.
14. Методический документ «Регламент включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России» (утв. Федеральной службой по техническому и экспортному контролю 26 июня 2018 г.). - 15 с.
15. Бачило, И. Л. Информационное право : учебник для академического бакалавриата М.: ЮРКОМПАНИ, 2017. – 292 с.
16. Васенин В., Шапченко К. Проблемы управления персональными данными // Открытые системы. 2019. № 9. С. 23-26.
17. Волчинская Е.К. Некоторые правовые проблемы применения Федерального закона о персональных данных // Персональные данные 2019. № 2. С. 56-61.
18. Гаврющенко А. П., Масленников А. В.. О методике определения актуальных угроз информационной безопасности с использованием БДУ ФСТЭК// Auditorium. 2022. № 2 (34) С. 37-43.
19. Комментарий к Конституции Российской Федерации /под ред. В.Д. Зорькина, Л.В. Лазарева. – М.: Норма, 2010. – 512 с.
20. Комментарий к Федеральному закону от 27 июля 2006 г. N 152-ФЗ «О персональных данных» / Т. А. Кухаренко. М.: Ай Пи Эр Медиа, 2016 – 250 с.
21. Малеина М.Н. Право на тайну и неприкосновенность персональных данных //Журнал российского права. 2010. № 11 С. 11-15.
22. Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика М.: Статут, 2011. - 134 с.
23. Полякова Т.А. Химченко А.И. Актуальные организационно-правовые вопросы трансграничной передачи персональных // Прав. Журнал «Высшая школа экономики». 2018. № 1. С. 113- 116.
24. Стрельников В. Персональным данным - особую защиту //эж-ЮРИСТ. 2013-С. 6-8.
25. Ульянов В. Персональные данные в России 2018 // Information Security. Информационная безопасность. 2018. № 5. С. 22-25.