МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ГОСУДАРСТВА И ПРАВА
Кафедра теории государства и права и международного права

Заведующий кафедрой
д-р. юрид. наук, профессор
О.Ю. Винниченко

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
магистра

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЛИЧНОСТИ В МЕЖДУНАРОДНОМ И РОССИЙСКОМ ПРАВЕ

40.04.01 Юриспруденция
Магистерская программа «Защита прав человека и бизнеса»

Выполнила работу студент 3 курса заочной формы обучения	Баева Наталья Олеговна
Научный руководитель к.ю.н.,	Лиц Марина Олеговна
Рецензент Генеральный директор ООО «Юридическая фирма «Лидер Консалт»	Засекина Елена Борисовна

Тюмень
2020

ОГЛАВЛЕНИЕ

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

ГПК РФ – Гражданский процессуальный кодекс Российской Федерации

АПК РФ – Арбитражный процессуальный кодекс Российской Федерации

ГК РФ – Гражданский кодекс Российской Федерации

УК РФ – Уголовный кодекс Российской Федерации

ФЗ РФ – Федеральный закон Российской Федерации

ФКЗ РФ – Федеральный конституционный закон Российской Федерации

РФ- Российская Федерация

ЕСПЧ- Европейский суд по правам человека

ЕС- Европейский союз

ЭВМ- Электронно-вычислительные машины

ИКТ- Информационно-коммуникационные технологии

ООН- Организация Объединенных Наций

ИТ- Информационные технологии

ИБ- Информационная безопасность

МСЭ- медико-социальная экспертиза

УКГВ- Управление по гуманитарным вопросам

УВКПЧ- Управление Верховного комиссариата по правам человека

ПРООН- программа развития Организации Объединенных Наций

ЮНЕП- программа Организации Объединенных Наций по окружающей среде

ЮНЕСКО- специализированное учреждение Организации Объединенных Наций по вопросам образования, науки и культуры

УВКБ- Управление Верховного комиссариата по вопросам беженцев

ЮНИСЕФ-Детский фонд Организации Объединенных Наций

ЮНОПС- Управление Организации Объединенных Наций по обслуживанию проектов

ВОЗ- Всемирная организация здравоохранения

ВВЕДЕНИЕ

Настоящая работа посвящена рассмотрению правовых проблем на международном уровне по вопросам защиты информационной безопасности личности.

Актуальность выбранной темы обусловлена тем, что на сегодняшний день традиционные методы государственного регулирования в современной информационной среде нередко оказываются незначительными в своей эффективности, особенно в тяжелое время пандемии, когда каждая личность особенно уязвима в век информационных технологий и раскрытия конфиденциальной информации через каналы связи интернет.

К учету вышесказанного, для исполнения международного сотрудничества органами власти, идет акцентирование на обеспечение защиты личной, конфиденциальной информации. Первоначально идея о создании единого правового режима защиты информационных данных была отражена в Концепции информационной защищенности Российской Федерации (Доктрине) и реализации задумок международной информационной безопасности, принятой положительно Межведомственной комиссией по информационной безопасности Совета Безопасности РФ.

В Конституции Российской Федерации закреплены права и свободы граждан и придается особое значение о неразглашении личной информации без согласия личности. Большое значение в наше нелегкое время имеет чувство защищенности для всех граждан, и каждый имеет право на безопасное существование и хранение личных данных, как в российской, так и в международной системе.

Согласно статье 24 Конституции Российской Федерации и приведенным комментариям к ней:

- в первом пункте акцентируется особое внимание на защите конфиденциальной информации. Каждое несогласованное информационное вмешательство в личные отношения ставит под сомнение достоинство

личности и придает значение охране данных об индивидуальном существовании личности, поскольку любое действие без согласования частного лица в области личных взаимоотношений, не только лишь умаляет преимущество персоны [Конституция РФ, ч.1, ст.21], подставляя под значительную угрозу право на неприкосновенность частной жизни, личной и семейной тайны [Конституции РФ, ст. 23, ст. 25], иным правам и свободам, связанным с само становлением [Конституция РФ, ст. 26, ст. 28, ст. 29, ст. 30 и др].

Само понимание и его преимущественный прогрессивный рывок в области правоотношений к неприкосновенности частной жизни, усилено примерами тоталитарного порядка XX вв., стремлением к полному контролю за частной жизнью, описанному в романе Дж. Оруэлла 1984 год.

Остро стоит данная проблема и в наше действующее время, так как с прогрессирующим изобретением и развитием программных средств наблюдения, которые позволяют анонимно вторгаться в частную жизнь, с развитием электронно-компьютерных систем и информационных сетей, способных накапливать, хранить и использовать неограниченные количества индивидуальных данных и не дающих абсолютных гарантий их сохранности, с повышением чисто коммерческой ценности любой информации, в том числе информации о частной жизни.

Право на частную жизнь, в том числе на информационное таинство, стоит на идее самоопределения и автономности личности, свободе индивида в приватной, интимной сфере его жизни от внешнего контроля со стороны государства и общества. «Конституция РФ, раздел 1, глава 2, стр 24»

В моей работе, посвященной информационной безопасности личности в международном и российском праве, исследования посвящены в свою очередь не только государственным отношениям, хотя по большей части я рассматриваю действия, направленные на защиту информационных данных, так и регулирование на международном уровне.

Изучая данную область, задаешься вопросом: «С чем связано такое увеличение «кибер- атак», «утечки» информации, и как в современном мире, мире нанотехнологий обезопасить свои конфиденциальные данные?» На сегодняшний день сеть интернет, такая всемирная паутина, невероятно охватила каждый уголок земного шара, еще лет 20-25 тому назад сложно было и представить о таких возможностях, как совершить покупку каких то вещей в одном уголке земного шара, и получить абсолютно в противоположном. Все это конечно замечательно, но не все и далеко не всегда задумываются о безопасности платежной системы и передачи своих личных данных.

Анализируя и выделяя информацию из множества доступных ресурсов, приходишь к следующему выводу: на данном этапе, если «встать на чашу весов» и начать балансировать между безопасностью личности и безопасностью информационно содержащих ресурсов с личными данными, ни государство, ни частное лицо в целом не откажется в предоставлении конфиденциальных данных, поскольку отторжение использования сети интернет уже, увы, не предоставляется возможным, в нашем современном мире. Остается задуматься «о безопасности соединения».

Более остро в настоящее время стоит проблема обеспечения сохранности данных в условиях, с которым столкнулись все без исключения, период нагрузки на все сети в режиме самоизоляции, где так же под угрозу попали данные принадлежащие не только мирным гражданам, но и организациям.

Степень научной разработанности темы. Правовые аспекты влияния информационных и коммуникационных технологий на развитие современного общества были исследованы еще в трудах Аграновской Е.В., Брусницына Н.А., Бачило И.Л., Карпычева В.Ю., Хижняк В.С., Черкасова В.Н., Романовского Г.Б. и другие.

Целью исследования является научно-исследовательская работа в области информационной безопасности личности в международном и российском праве.

На основе исследований и анализа существующих проблем разработки теоретических, правовых и нормативных требований, практические положения, предложения и рекомендации, направленные на эффективность продвижения международных и российских прав в области информационной безопасности и особенности безопасности личности.

Для достижения раскрытия поставленного вопроса были сгруппированы задачи:

1) рассмотреть и раскрыть понятие «информационная безопасность личности» в Международном и российском праве

2) рассмотреть и раскрыть эволюцию понятия «международная защита» на основе анализа Международных договоров

3) раскрыть историческую взаимосвязь

4) провести сравнительный анализ информационной безопасности личности в Международном и российском праве

5) обозначить и решить проблему информационной безопасности личности

6) обозначить и решить проблему информационной безопасности в условиях пандемии

7) сформулировать предложения по изменению регулирования защиты информационных данных личности.

Редко встретишь ученых, чьи позиции схожи в данных вопросах, в литературе часто высказаны различные точки зрения, объясняющие природу происхождения понятий, также предложено множество концепций, но одной и общей позиции по многим вопросам на сегодняшний день просто не существует.

Методологическая и теоретическая основа данного исследования. Методологическая часть исследования составил диалектический метод

познания, метод анализа и сравнения, метод обобщения, логический, исторический, историко- правовой, логический, формально-юридический.

Структура работы обусловлена целью и задачами и состоит из введения, двух глав, включающих четыре параграфа, а также заключения, библиографический список.

ГЛАВА 1. ТЕОРЕТИКО- ПРАВОВЫЕ ОСНОВЫ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА ПО ВОПРОСАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

1.1.ИСТОРИЧЕСКИЕ АСПЕКТЫ В МЕЖДУНАРОДНОМ ПРАВЕ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

Затрагивая исторические моменты можно углубиться и рассмотреть историю развития информационной безопасности начиная с момента за 220 лет до настоящего времени, и разделить их в порядке приближения на семь этапов, учитывая особенность развития распространения информации.

Первые упоминания о защите информации можно отнести к моменту, когда появилась письменность и общение между людьми за счет передачи писем.

И это не только относится к международным историческим моментам, но и к российским.

Начиная с событий до 1816 года - задачами по защите информации, отнесенными к этому периоду, можно назвать более естественными, так как главное, на что стоило акцентировать внимание, являлась защита информации в происходящих и произошедших моментах, хранящих исторические события: данные об имеющемся имуществе, ценных бумагах, местонахождении личности, прочие данные, имеющие важную личную информацию.

В дальнейшем, по мере развития и достижения человечества, следует отметить второй этап в истории развития, от 1816 года - это важная часть, где свое преимущество имеет развитие технического прогресса, а именно развитие радиосвязи и электросвязи.

Для передачи ценной информации на расстояния и обеспечения ей безопасности, нужно было изобрести шифрование, в противном случае

ценная информация могла «утечь», плюс ко всему для безопасности предоставления информации нужно было не допустить помехи, чтобы не исказить важные данные.

После методов «проб и ошибок» можно перейти к следующему этапу, начиная с 1935 года. С этим этапом связан прогресс, а именно достижение успехов в области радиолокаций и гидроакустики. Обеспечить информационную безопасность с проявлением прогресса уже было чуть сложнее. Единственным способом обеспечения безопасности на данном этапе было строгое соблюдение правил организационных моментов и технических мер.

В дальнейшем идут этапы развития компьютерной технологии, с 1946 года, изобретением первых электронно-вычислительных машин. На этом этапе защитить конфиденциальную информацию было проще, чем сейчас, достаточно было ограничить доступ к данным машинам.

В 1965 году, появилась первая локальная сеть. С защитой информации еще в эти года можно было справиться физическим воздействием, ограничив администрирование сети, но вот уже с 1973 года воздействовать на безопасность становилось все сложнее, так как появились мобильные коммуникационные устройства, развитие программ и устройств. На первых порах не составляло сложность в заимствовании информации, данных, что могло нанести урон на государственном уровне. С этого этапа можно выделить первое формирование информационного права - это новая ветвь в международной правовой системе.

И уже на последнем этапе, а именно с 1985 года, связанный с появлением глобальной сети «интернет», принято решение, под воздействием широкого уровня форумов, о создании защитного программного обеспечения и дало началу создания макросистем для информационной безопасности личности.

Каждый год страны, из-за несовершенства системы защиты информации, теряют миллиарды долларов.

Как последующий, новый этап, в истории становления можно выделить период с 1998 года, когда РФ впервые вынесла «проект резолюции» в комитет Ассамблеи, рассмотрев который приняли сразу же, без голосования.

С этого момента на ежегодной основе представители государств обязаны представлять отчет по этому вопросу.

С того года созданы компетентные группы лиц, занимающиеся вопросами реальных и возможных сетевых угроз, и на основе отчетов разрабатываются действенные меры по борьбе с ними.

Впервые зафиксировали успешный информативный отчет в 2010 году. Последующие доклады, изучавшие угрозы, разрабатывали меры исходя из отчета 2010 года.

В рекомендациях указываются действия, как увязать вопросы безопасности ИКТ с существующим международным правом и соглашениями, регулирующими межгосударственные отношения, служащими основой международного мира и безопасности.

В 2013 году, на основе результатов и отчетов за предыдущие года, принята резолюция и скооперирована новая группа экспертов для представления доклада Генеральной Ассамблее в 2015 году. В 2014 году в созданную группу избрали Бразилию председателем и состоялся последний доклад по теме информационной безопасности.

К этапу 2010 года можно соотнести события, связанные с разоблачением Сноудена, где выявлен вирус, поразивший систему иранской Атомной электростанции. Это говорит о том, что любая система имеет слабые места, и при желании и высоких знаниях можно их найти.

В дальнейшем можно создать или соотнести к истории новые обороты для информационной защиты данных личности, а именно выделить как отдельный этап, захвативший уже весь мир, этап пандемии.

Поначалу, когда поступила первая информация о заражении, многие отнеслись к этому скептически, и даже не восприняли всерьез, никто и подумать не мог о таком масштабе. Большинство расценивают это как

третью мировую войну, которую в принципе ожидали. Но, как показала практика, ни одно государство не было к этому готово во всеоружии.

Большой урон мировой экономике нанесли последствия данного вируса из-за нагрузки всей системы и неготовности к такой массовой защите данных, которое дало много «лазеек» для совершения преступной деятельности.

При переходе в режим «самоизоляции» и введении «комендантского часа», человечеству, как и государству в целом, пришлось практически полностью перейти на бесконтактную систему существования.

На международном уровне, к этому испытанию, более подготовлены частные лица, так как многие страны за рубежом давно перешли на бесконтактные рыночные отношения. Соответственно повторюсь, что методом «проб и ошибок» зарубежные страны более подготовлены.

Конечно, я не хочу сказать, что международная защита выполняется на сто процентов, ведь с развитием рыночных отношений, развиваются и вредоносные программы.

Рассмотрим международную практику в данном вопросе. Если исходить из источников информации в данной области вопроса, изучив исследования, склоняюсь доверять работе Мельникова В.П., объединившего в своих трудах мнения многих ученых, описав в книге: «Исследование систем управления». В его книге сказано о первом отчете, опубликованном агентством компьютерной безопасности Министерства обороны Соединенных Штатов Америки, в 1983 году, в котором разделили уровни и разработали инструкцию оценки компьютерных систем.

Последователями, озаботившимися об информационной безопасности, стали представители Германии в данной области, которые, в свою очередь, уже выдвинули требования к доступности информации.

Данные требования («Зеленая книга», в цвет переплета) в 1990 году были одобрены Германией, Великобританией, Францией и Голландией и направлена в ЕС, где была подготовлена схема действий, в которой есть

определенные условия дающие гарантию на безопасность в информационной системе, имеющие два алгоритма проверки: по эффективности и по функциональности. К этим критериям, в свою очередь, добавили элементы, которые их характеризуют, цели и функции информационной безопасности, их особенности, способы идентификации и аутентификации, управление правом доступа [Лопатин, 48с].

В исследовании ученого можно также прочитать информацию, что помимо «зеленой книги», до этого было издано еще две по цвету переплета, красная и белая, в которых разрабатывались стратегии безопасности информационных данных.

В последующих разработках увеличивалось число критериев и оценок безопасности системы, в конечном итоге было принято объединить и создать общие критерии, которые дают оценку защищенности и устанавливают требования к функциональным возможностям и гарантиям; несколько этапов, гарантирующих защиту данных, которые может запросить пользователь; два понятия: «профиль защиты». [Мельников, с190-192]

Изучая исторические моменты, в своей работе я решила проанализировать первый международный акт, касающийся защиты информационной безопасности личности.

Своим истоком, относящимся к защите персональных данных, можно соотнести первый документ, который указан еще в 1981 году.

В ходе поисков по различным источникам предоставления информации, первый документ: «Конвенция о защите физических лиц при автоматизированной обработке персональных данных» (Заключенная в Страсбурге 28.01.1981) (Поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных, «позволяющими присоединение европейских сообществ, утвержденные Комитетом Министров в Страсбурге 15.06.1999) Она была принята Госудумой 25 ноября 2005 года и одобрена Советом Федерации 7 декабря 2005 года.

В данной Конвенции проработаны вопросы, которые относятся непосредственно к международной правовой защите по персональным данным. В данный документ были внесены и поправки, но уже спустя 11 лет.

Утвердить Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года с поправками, внесенными комитетом министров Совета Европы 15 июня 1999 года, подписанную от имени Российской Федерации в Страсбурге 7 ноября 2001 года, с последующими поправками: РФ сделали несколько заявлений с не применением пп «А, В» п. 2 ст. 3 Конвенции по отношении к личным данным; согласно пп «А» п. 2 ст. 9 РФ имеет полное право устанавливать ограничения на доступ к личным данным.

Данная Конвенция не имеет оговорок, согласно статьи 25 Конвенции, и согласно статье 27 написана на двух языках (английский и французский), которые воспринимаются идентично, оригинал в одном количестве помещен в архив Совета Европы. Копии этого документа отправлены каждому, приглашенному присоединиться к настоящей Конвенции. Как и во многих документах при переводе преобладает английский язык.

Если говорить по историческим аспектам, то следует сделать вывод, что неотъемлемо растет развитие общества в области информационных технологий, и направленность государства на решение конфликтных ситуаций в информационном потоке, прилагает максимум усилий для недопущения вмешательства сторонних в частную жизнь и государственные вопросы. Но следует учесть, что при развитии технологического прогресса в области информационной технологии, также развивается и преступный фактор, и порой с изобретением новых программ, казалось, для упрощения оформления тех же заказов товаров или услуг, образуются слабые стороны в алгоритме, что предоставляет потенциальный доступ к информации. На различных этапах развития технологий, следует вносить поправки в законодательство и учитывать риски возникновения конфликтных ситуаций.

К примеру, все новые проекты с использованием ИКТ, должны проходить регистрацию и получать разрешение на вид деятельности, соответственно, должны приобретать лицензии и программное обеспечение по защите данных, и прочие схемы действий для возможности существования на информационной платформе. Я считаю, что принцип работы с данными и защита их, должна иметь единый международный стандарт, так как в той или иной степени торговые отношения сейчас действуют для всех, соответственно и работать должны по единому стандарту, и метод контроля должен быть разработан в едином стандарте.

1.2. ЭВОЛЮЦИЯ ПОНЯТИЯ МЕЖДУНАРОДНОЙ ЗАЩИТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

В данной главе, в своем первом пункте мы кратко рассмотрели исторические моменты касающиеся информационной безопасности личности, но ни в одном из пунктов нет конкретного понятия «международная информационная защита безопасности личности», рассмотрим подробнее.

Раньше под «защитой информации» было понято уважение прав и свобод человека.

В дальнейшем при изучении данного вопроса выявилось, что четкого определения нет, но в научной литературе используют обширное, не имеющее четкой формулировки, но схожее по смыслу, определение.

Ученые по данному вопросу высказываются по разному, кто-то, допустим, думает, что совокупность вопросов в данной области включает соглашения между государствами и вхожие в него документы. Есть и другие наблюдения: вопросы международной защиты подразумевают создание межгосударственных соглашений и соответствующих документов по правам человека. Есть еще мнение, что «международная защита» как некая международная солидарность в соблюдении прав и свобод человека.

Взаимодействия по «международной защите» прав личности включает: «создание многоцелевой документации по правам индивидуальности человека; модернизации межгосударственных сотрудничеств в данной сфере; модернизации дополнительного механизма для мониторинга выполнения государствами данных всемирных обязательств в сфере прав человека» [Мовчан, с. 74]

Имеется еще такое мнение, что понятие «международная защита в сфере прав человека» является совокупностью принципов и норм, составляющих одно из направлений современного международного права».

Юрист С. В. Черниченко изначально понимал, как действия государств по борьбе с грубыми и массовыми нарушениями прав человека. Но по прошествии времени поменял мнение о понимании международной защиты прав человека и утверждает, что оно значительно приняло новый оборот. [Черниченко, с. 9].

Людмила Павловна в одной из своих статей пишет: «она это даже подчеркивает, что одни авторы рассматривают международную защиту как компонент международного сотрудничества в сфере прав человека, другие сводят ее только к деятельности межгосударственных контрольных органов, а третьи включают в этот термин разработку рекомендаций, межгосударственных стандартов, обязательных для государств, и контроль за их применением». [Павлова, с. 24]

В различных научных источниках понятия трактуются по-разному и единого мнения нет, написано множество статей с исследованием данного вопроса, где на международном уровне, данное понятие рассматривают соотнося к нему защиту от кибер угроз. В исследованиях российских ученых больше применяется терминология, связанная с широким понятием, включающая технические достижения, безопасность сетей, манипулирования информацией и воздействия над ней.

Исходя из приведенных доводов, можно считать более приближенным, обобщенное мнение, в связи с чем термин можно определить как «система международных органов и процедур универсального и регионального характера, работающих в направлении разработки международных стандартов в области прав и свобод человека и контроля за их соблюдением государствами». [Павлова, с. 25]

Среди определений можно отметить «Международная безопасность» — это состояние защищенности национальных интересов государств того или иного региона мира от угроз общего характера. «К подобным угрозам относятся распространение ядерного терроризма, глобальные экологические угрозы и т. п.». [Фролов, с. 56]

В Концепции Республики Беларусь, утвержденной 18.05.2019г. «Об информационной безопасности», в третей главе, есть более подходящее определение «международной информационной безопасности» - состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве.

Скорее всего это более близкое по смыслу определение, подходящее под масштабы его значения, но все таки оно не имеет статуса утвержденного и конкретизированного.

Из вышесказанного видно, что данное понятие со временем не конкретизировалось, а обрастало новыми терминами, дающими более обширное понимание.

Под международной информационной безопасностью, согласно терминологии ООН, понимается защищенность глобальной информационной системы от террористических, преступных и военно-политических угроз. В 2003 году Россия в документе «Основы государственной политики в области международной информационной безопасности до 2020 года», также в качестве международных угроз обозначила опасность вмешательства во внутренние дела суверенного государства посредством информационно-коммуникационных технологий. Такой тип угроз опасен возможностью нарушения общественной стабильности, а также разжигания межэтнической и межнациональной розни. Чаще всего она понимается как столкновение национальных интересов государств, однако в целом вопрос терминологии остается дискуссионным.

Россия придерживается широкого понимания термина «международная информационная безопасность», являющегося собирательным различных технических аспектов, включая безопасность информационных сетей и систем, а также манипулирование информацией, ее распространение путем глобальных информационных сетей и информационного воздействия. При этом страны Запада и, прежде всего, США являются сторонниками узкого

подхода, понимая под международной информационной безопасностью только технические аспекты и кибербезопасность.

Следует учитывать, что каждое определение в различных источниках информации, законодательных документах, исследований ученых, по-своему является истиной, но ввиду неточности, а лишь использования нескольких определений, собранных воедино.

Следует сделать вывод, что понятие «международная защита информационной безопасности» подверглось различной интерпретации, с 1983 года в него входили межгосударственные отношения, не противоречащие глобальным интересам в области информации, которые закреплены в международном праве. С развитием информационных технологий, в данное понятие вкладывали обширное значение, но одно могу сказать, что четкого определения «международная защита информационной безопасности» отсутствует и весомые аргументы приведены выше.

В моем понимании можно сделать заключение и дать определение, что входит в данный смысл выражения «международная защита информационной безопасности личности» - это совокупность систем и процедур различных международных органов, в чьих интересах на первом плане идет защита личных данных, «международных стандартов в защите прав человека», разработка единого механизма соблюдения контроля за выполнением стандартов государствами.

ГЛАВА 2. ПОНЯТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ В РОССИЙСКОМ ПРАВЕ

2.1. АНАЛИЗ РОССИЙСКОГО ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИОННЫХ ДАННЫХ ЛИЧНОСТИ

Наше Государство на протяжении почти 27 лет чтит и соблюдает Основной Закон Российской Федерации (Конституция РФ). Исходя из свода целей, задачей, взглядов, направлений на информационную безопасность, основой понимания в данной области следует чувство защищенности, как многонациональных интересов, так и личности, государства и общества в целом.

Если говорить о российском праве, в области правосудия по данному вопросу, то можно выделить момент, что исполнители или, по-другому, органы местного самоуправления, и те, кто к ним относятся, не вправе скрывать документацию и сопутствующие к делу элементы от заинтересованного лица, если это касается «прав и свободы, конечно, если нет оговорок» и если иное не предусмотрено законом.

Известны случаи обращения в суд (Конституционный Суд РФ) по вопросам, сутью которых является отказ в предоставлении их процессуальных и профессиональных прав на получение информации (положениями закона № 152-ФЗ). Желание добиться справедливости в данном вопросе, как правило, приводит к вопросам по ограничению прав защищающей стороны и, как правило, непосредственного присутствия в заседании (определение от 29 января 2009 г. N 3-О-О).

Данное понятие в определении не дает сомнения в особом правовом режиме, содержащем персональные данные.

Был опыт, что по основному документу (Конституция Российской Федерации), ограничивали права на получение информации по делу, и он

соответствовал законодательству (ч. 2 ст. 24 Конституции Российской Федерации).

По-другому, под опасность попадало право на неприкасаемость к индивидуальной жизни (обеспеченное частью 1 статьи 23 и частью 1 статьи 24 Конституции).

Резюмируя вышесказанное, руководствуясь занимаемой позицией, суд (Конституционный Суд РФ) подтвердил, что Федеральный закон (от 22 декабря 2008 г. N 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации») не «воздействует на взаимоотношения, имеющие отношения» к обеспечению доступа к информации о деятельности судов, «имевшие персональные данные» (определение от 16 декабря 2010 г. N 1626-о).

Но стоит учесть, что это правило не подразумевает абсолютного запрета на доступ к любой информации, содержащей индивидуальные данные.

Те, кто имеют право на доступ к индивидуальным данным, должны быть перечислены в законе, но есть некая оговорка, что законодатель официально не включил адвокатов в их число (определение от 17 июня 2008 г. N 434-о-о).

В законодательстве (ч. 2 ст. 24 Конституции РФ) представлен порядок и определенные условия обеспечения гарантированных прав, имеющих место быть в компетенции федерального законодателя, в котором, исходя из этого, вправе представлять различные требования к гарантиям и степени возможных условий на представления информации при условии адекватности таких ограничений конституционным требованиям, если их введут в эксплуатацию (ч. 3 ст. 55 Конституции РФ).

При этом, как обозначил Конституционный Суд РФ (в постановлении от 18 февраля 2000 г. № 3-п, ограничение права, вытекающего из ч. 2 ст. 24 Конституции РФ), предоставляется только в полном соответствии с законом, дающий особый правовой статус информации, ограничивающий право на распространение, ввиду ее содержимого, а также присутствие информаций, которые можно соотнести к государственной тайне, индивидуальной

информации, служебной и/или коммерческой тайне, профессиональной и изобретательской деятельности.

Также соблюдается коммерческая тайна по прошению, Федеральный законодатель не называет адвокатов в числе лиц, и сведений связанных с персональными данными.

По основному документу (ст. 23 Конституции РФ) обеспечивает в полном объеме право на секретность информации «об общении и не только».

«В предоставлении неверной информации, которая порочит имя и моральные ценности как личности, имеются правозащитные меры (ч 1 ст 23 Конституции РФ)», где четко прописано о праве гражданина на защиту своей чести и своего доброго имени. Но следует помнить о понятии «доброе имя», что далеко не все имеют безупречную репутацию.

Но вопросы о безупречной репутации существуют до тех пор, пока судом не докажут обратное. Защитить свое «доброе имя» можно, как физическим лицом или группой лиц, так и общественной организацией или юридическим лицом, которые связаны с частным лицом и пострадали в результате клеветы, оскорблений или распространения иной порочащей честь и достоинство информации.

В законодательстве устанавливается право на свободу слова и свободу мысли, на расположении имеющейся информацией (Ст. 29 Конституции РФ). Трактовка настоящей статьи подразумевает демократическое государство, признающее многообразие мнений. Но, может быть, эта статья имеет больше ограничений, если проанализировать. Это не спроста, так как свобода мысли и слова не может быть абсолютной.

Если говорить обобщенно, то ограничения сформулированы в законе (Ст. 55 Конституции РФ). Кроме того, ГК РФ, АК РФ, УК РФ возлагают наказание за публичные призывы к террористическим актам и т.д.

В современных условиях, очень часто, обобщенным, предоставляется создание информационных носителей, серверов, соответствующими законодательными, исполнительными и судебными органами и создает

условия к доступности, актуальности и целостности предоставляемой на них информации, то есть обеспечение информационной безопасности.

В документе (Указе Президента Российской Федерации от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации») есть немаловажные стороны, представляющие национальные интересы в данной сфере: обеспечение прав, соответствующих конституционным нормам, механизмам, поддержки со стороны законодательства и обеспечение их выполнения; чувство защищенности и пребывание в мирное время с обеспечением выполнения всех норм; совершенствование системы, как в развитии прогресса технологических систем, так и в разработке программного обеспечения по ее защите; защита достоверности предоставляемой информации; формирования и создания правовой защиты интересов общества в направлении информационной безопасности".

Если говорить о приведении в действо общенациональных интересов в информационной области, нацеленных на реализацию в структурировании и обеспечении надежной среды кругооборота правдивой информации и стабильной к всевозможным критериям влияния информационной инфраструктуры для предоставления законодательных прав и свобод человека, стабильного социально- экономического становления страны.

Говоря о приоритетах (Согласно р. 23 Указа Президента РФ от 5.12.2016 года № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации») ИБ, в разрезе государственной и социальной защищенности, то «противодействие применению информационных нанотехнологий в задачах к агитации террористической идеологии» главной задачей которых стоит подрыв суверенитета, политической и социальной незыблемости, экстремистского преобразования конституционного строя, расшатывание интереса региональной неделимости РФ».

Соглашаясь со всем этим, вперед можно выдвинуть действие об усовершенствовании российского законодательства. А также стоит уделить особое внимание о выдвижении законов, имеющих отношение к устранению сетевой преступности.

К ним относятся такие, как: закон Российской Федерации «О государственной тайне» от 21.7.93 г. № 5485-1, закон РФ «О коммерческой тайне» (редакция 28.12.94 г.), Закон РФ «Об информации, информатизации и защите информации» от 25.1.95 г., Закон РФ «О персональных данных» (редакция 20.02.95 г.), Закон РФ «О федеральных органах государственной связи и информатизации» от 19.2.93 г. 4524-1. Положение о государственной системе защиты информации в Российской Федерации от ИТР и от утечки по техническим каналам. (Постановление Правительства Российской Федерации от 15.9.93 № 912-51), Положение о государственной технической комиссии при Президенте Российской Федерации (Государственная техническая комиссия России). Указ Президента Российской Федерации от 28.12.92 № 829-РПС.

В Уголовном кодексе Российской Федерации в главе 28 преступления в области компьютерной информации» содержатся статьи 272, 273 и 274: несанкционированный доступ к компьютерной информации (подразумевается внедрение без согласия в индивидуальность жизни личности); создание, использование и распространение вредоносных компьютерных программ (подразумевает контакт с вирусоносным обеспечением); нарушение правил эксплуатации компьютеров, компьютерных систем или их сетей (подразумевает нарушения в доступности и сохранности информации, которые обычно подводят к уничтожению, блокированию или модификации охраняемой законом).

Статья 138 Уголовного кодекса Российской Федерации, обеспечивающая защиту персональных данных», подразумевают ответственность за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Идентичную защитную роль в

финансовой тайны предоставляет статья 183 Уголовного кодекса Российской Федерации.

Большим минусом, хотелось бы отметить, доверчивость людей. Порой в хищении информации и/или денежных средств со счетов из приложений, или с той же самой карты, виноваты сами же обладатели конфиденциальной информации, так как постороннему лицу, сами того не подозревая, дают так называемый «ключ» к информации.

В текущий момент участились случаи хищения денежных средств со счетов клиентов, и в основном, по вине держателей карт.

Недаром в документах и при оформлении банковского продукта, сотрудники банка предупреждают своих клиентов о важности конфиденциальных данных, которые ни при каких обстоятельствах никому нельзя сообщать, тем более по телефону.

На картах также указаны только официальные номера телефонов того или иного банка.

Но в настоящий момент все больше и больше заявлений поступают от потерпевших, в которых говориться, что по незнакомому номеру сами же их разгласили.

Я считаю, что в наше время, каждому клиенту, необходимо выдавать небольшие, доступные к восприятию, памятки по подобным ситуациям.

Утечка персональных данных может произойти практически из любой организации. Однако в серьезных, богатых, длительное время существующих организациях такая вероятность меньше, а возможностей исправления ее последствий - больше.

Поэтому первая рекомендация - не передавайте персональные данные в организации, в которых вы не уверены. Прежде всего, речь идет о неизвестных вам интернет- магазинах и интернет-сайтах.

Вторая рекомендация - никогда не пересылайте фотографии, копии своих паспортов, банковских карт неизвестным вам лицам и тем, в ком вы недостаточно уверены.

Третья рекомендация - при пересылке личных данных в знакомые вам организации пользуйтесь официальными ящиками электронной почты, указанными на официальном сайте.

Четвертая рекомендация - фиксируйте в специальном списке все созданные вами аккаунты в социальных сетях, личные кабинеты, сайты, на которых вы регистрировались. Периодически проводите ревизию этого списка. Закрывайте все аккаунты, кабинеты, регистрации и т.п., которыми вы не пользуетесь.

Пятая рекомендация - при посещении организаций, где при входе требуют предъявлять паспорт и фиксируют паспортные данные, старайтесь паспорт показывать, но не передавать работникам службы охраны в руки. Желательно, чтобы вы сами заполняли формуляры со своими паспортными данными.

Необходимо также с осторожностью относиться к социальным сетям.

Порой, выкладывая на всеобщее обозрение, сами того не подозревая, мы предоставляем злоумышленникам огромный поток информации для ее использования в негативных целях.

Использование фотографий может обернуться к последствиям утрат с финансовой стороны. Это сейчас уже известно, по опыту других пользователей, что если тебе пишут с аккаунта твоего знакомого и просят дать в долг не великую сумму, то это вызывает подозрения. Но этот опыт мы приобрели ввиду понесенных потерь.

Интересы правительства в области предоставления защиты недоступности информации более точно оговорено в законе «О государственной тайне» (в редакции от 6 октября 1997 года). В котором дается определение «государственной тайны» выраженной в информации, обеспеченной защитой государством в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной сфере деятельности,

огласка которой определенно может нанести вред в обеспечении безопасности Российской Федерации.

В свою очередь он обеспечивает рычаги информационной безопасности. Следуя данному закону, это технические, криптографические, программные и иные средства, предназначенные для защиты информации, составляющей государственную тайну; средства, в которых они осуществляются, а также средства контроля эффективности защиты информации.

Фундаментальным среди российских законов об ИБ можно учитывать закон «Об информации, информатизации и защите информации» от 20 февраля 1995 года (принят Государственной Думой РФ 25 января 1995 года; действующая редакция закона от 21.07.2014 года). В нем даются базовые значения и обозначаются направления развития законодательства.

Ниже приведены примеры таких определений:

- информация — сведения о лицах, объектах, фактах, событиях, явлениях и процессах, независимо от формы их представления;

- документированная информация (документ) — информация, записанная на материальном носителе с реквизитами, позволяющими ее идентифицировать;

- информационные процессы — процессы сбора, обработки, накопления, хранения, поиска и распространения информации;

- информационная система — это организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы;

- информационные ресурсы — отдельные документы и отдельные массивы документов, Документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных и других информационных системах);

- сведения о гражданах (персональные данные) — сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;

- конфиденциальная информация — документально подтвержденная информация, доступ к которой ограничен в соответствии с законодательством Российской Федерации;

Законом предоставлена сама суть защиты информации: предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение угроз безопасности личности, общества и государства; предотвращение несанкционированных действий по уничтожению, изменению, искажению, копированию и блокированию информации; предотвращение иных форм незаконного вмешательства в информационные ресурсы и информационные системы, а также обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах; сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законом; обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Если резюмировать данный закон, то следует сказать о том, что любые манипуляции с информацией, имеющей отношение к конфиденциальности, без согласия собственника, являются противозаконными.

Следуя закону, охране на законодательном уровне подлежит любая документально удостоверенная информация, которая может нанести вред ее правообладателю, владельцу, пользователю или иному лицу.

Режим защиты информации устанавливается в отношении сведений, отнесенных к государственной тайне, уполномоченными органами на основании закона Российской Федерации «О государственной тайне»; в

отношении конфиденциальной документированной информации-владельцем информационных ресурсов или уполномоченным лицом на основании настоящего Федерального закона; в отношении персональных данных — Федеральным законом.

Отсюда следует, что на законодательном уровне, прилагаются максимальные усилия для обеспечения безопасности данных личности.

Стоит акцентировать внимание на то, что государственная тайна и персональные данные охраняются государством, а иная секретная информация приходится во владении ее правообладателя.

В качестве безопасности систем, любые носители и хранители информации должны обладать соответствующей лицензией, либо иметь сертификат.

В качестве базового механизма защиты информации закон предоставляет многофункциональные инструменты — лицензирование и сертифицирование (статья 19): информационные системы, базы данных и банки данных, предназначенные для предоставления информационных услуг частным лицам и юридическим лицам, должны иметь сертификат, в соответствии с законом РФ «о сертификации продукции и услуг».

Информационные системы органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации, других государственных органов, организаций, совершающих обработку документальной информации с ограниченным доступом, а также средства служащие для безопасности этих систем подлежат обязательной сертификации.

Порядок проведения аттестации определяется законодательством Российской Федерации.

Организации, выполняющие работы в области проектирования, производства средств защиты информации и обработки персональных данных, получают лицензии на определенный вид деятельности.

Порядок лицензирования определяется законодательством Российской Федерации.

Интересы потребителя информации при использовании импортной продукции в информационных системах защищаются таможенными органами Российской Федерации на основе международной системы сертификации.

Для приобретения сертификатов или предоставления сертификатов, есть существенно значимые требования в законе.

Касаемо законодательства (п.2,3,4,5 ст 22):

- правообладатель, работающий на платформе с характерным документом или целым пакетом, имеет полное право запросить сертификат и получить характерную помощь.

- правообладатель документов, работающий на платформе должен знать обо всех действиях направленных на нарушение режима ИБ.

Статья 23 под п.2,3,4: «защита прав субъектов в области информационных процессов и информатизации», в которой говориться: защищенность прав субъектов в данной области обеспечивается судом, третейским судом, третейским судом с расчетом тонкостей нарушений и нанесенного вреда.

Весомость имеют пункты статьи 5, имеющие соприкосновения с указанными, юридически весомыми документами, находящиеся в электронном виде и подписаны электронной цифровой подписью.

Юридический вес документа, над которым проводятся манипуляции с помощью автоматизированных информационно-телекоммуникационных систем, приобретает если подтвердить электронной цифровой подписью.

В наше время ЭЦП имеет юридическую силу, как и синяя подпись собственника, если имеется программное обеспечение, которое может обеспечить идентификацию данной подписи в установленном режиме.

ЭЦП запросто можно проверить на подлинность программным обеспечением, а вот уже сам порядок выдачи лицензий определяется законодательством Российской Федерации.

Тут уже большую роль играют положения Закона «Об информации, информатизации и защите информации», имеющие отношения к защищаемой информации и ИБ.

Больше всего меня затронуло то, что на международном уровне изначально для обеспечения ИБ планировалось создать чуть ли не военное положение, Россия же в свою очередь за мирное урегулирование, за то, чтобы решать все вопросы на законодательном уровне.

Соприкоснувшись с ИБ, рассмотрено несколько примеров практики ЕСПЧ.

1. Постановление ЕСПЧ от 28 мая 2019 года по делу "Сидорова против Российской Федерации" (жалоба N 35722/15).

В 2015г. по делу успешно рассмотрена жалоба на получение органами полиции конфиденциальной информации о психическом состоянии заявительницы. По делу допущено нарушение требований статьи 8 Конвенции о защите прав человека и основных свобод.

В своей жалобе Заявительница жаловалась на получение органами полиции конфиденциальной информации о ее психическом состоянии и это являлось нарушением ее прав на защиту частной и личной жизни.

28 мая 2019 года, по в жалобе, поданной заявителем, Европейский суд единогласно постановил, что в данном случае власти Российской Федерации нарушили требования статьи 8 Конвенции (право на уважение частной и семейной жизни), и обязал государственные органы-ответчики выплатить заявителю 5000 евро в качестве компенсации морального вреда и 1140 евро в качестве компенсации судебных издержек и издержек.

Суть данной практики показывает, что на уровне российского законодательства мы имеем защиту персональных данных, но у нас нет достаточных ресурсов обеспечивающих исполнительность постановлений, в

связи с чем, заявительнице пришлось обратиться в ЕСПЧ, и отстаивать свои права. К информационной безопасности из данной практики относится нарушение статьи 8 Европейской Конвенции о защите прав человека, а именно сбор информации медицинского характера, без согласия правообладателя.

2. Дело «Авилкина и другие (Avilkina and Others) против Российской Федерации» (Жалоба N 1585/09) Постановление Суда Страсбург, 6 июня 2013 г.

Дело было инициировано жалобой N 1585/09, поданной против Российской Федерации в Европейский Суд по правам человека (далее - Европейский Суд) в соответствии со статьей 34 Конвенции о защите прав человека и основных свобод (далее - Конвенция) Управленческим центром "Свидетели Иеговы" в России в лице его председателя Василия Михайловича Калина (далее - центр-заявитель) и тремя гражданками Российской Федерации: Екатериной Сергеевной Авилкиной, несовершеннолетней, интересы которой представляла ее мать Елена Николаевна Авилкина, Ниной Николаевной Дубининой и Валентиной Алексеевной Жуковой (далее - первая, вторая и третья заявительницы соответственно), - 19 декабря 2008 г. Заявители, в частности, утверждали, что раскрытие их медицинских документов прокуратуре составляло нарушение их права на уважение личной жизни, плюс из материала дела запросили компенсацию расходов, на веских основаниях Суд единогласно признал жалобу на нарушение ст. 8 Конвенции и ст.14 в совокупности к ст.8 Конвенции в части передачи медицинских данных.

По сути, к информационной безопасности, тут имеет отношение нарушение статьи 8 Конвенции, также как и в первом примере, в данном варианте идет раскрытие информации медицинского характера, без согласия правообладателя.

3. 16 июля 2020 г. Суд Европейского союза принял решение по делу Schrems II.

Благодаря решению суда социальные сети не могут передавать конфиденциальные данные в коммерческих целях, и на решение повлияло законодательная база США, в которой защищают права человека от избыточного пользования. Ко всему прочему, суд удостоверил условия договора, который был утвержден Европейской комиссией, для передачи персональных данных из ЕС в страны, согласные с правом ЕС, не внушают уверенность в защите прав касающихся персональных данных.

Одно из самых интересных дел, в практике ЕСПЧ, я считаю. Вся суть в том, что нарушен порядок обмена данными между ЕС и США.

Во второй раз менее чем за пять лет Европейский Суд установил, что соглашение об обмене данными между ЕС и США не соответствует стандартам защиты данных ЕС. Соглашение о «Безопасной гавани» было расторгнуто в 2015 году и было быстро заменено на «Защитный щит», теперь оно тоже летит в клочья. Суд правил что для того, чтобы быть действительным, соглашение ЕС / США должно предусматривать меры защиты, эквивалентные тем, которые гарантированы Общим регламентом о защите данных ЕС, и защиту права на неприкосновенность частной жизни и защиту данных, которые закреплены в статьях 7 и 8 Хартии основных принципов ЕС.

Суд также отметил в своем решении вопрос, касающийся российских партнеров, к которым попадают персональные данные от ЕС, использующие положения договора:

1) защита полученных персональных данных, оговариваемая в договорных соглашениях, должна быть обеспечена с теми же условиями и на том же уровне, что и хранящаяся в ЕС, полученная от партнеров.

2) критерии уровня защиты данных должны соответствовать законодательству и принятым международным соглашениям.

3) если, при передаче данных, существуют веские основания полагать, что персональным данным не будет обеспечена защита и договорные

отношения подвергаются сомнению в условиях их соблюдения защиты, то уполномоченные страны могут приостановить передачу данных.

Суть данной практики заключается в следующем: обнаружили, что социальная сети фейсбук, использовали данные в свое усмотрение, а именно, данные пользователей передавались по запросам иностранным государствам, что нарушало права человека. В связи с нарушением обмена данных между ЕС и США, обеспечение передачи данных партнеров ЕС с Россией, многих подвергает в сомнение, так как в свете последних событий, существует информация, что в нашей стране не должным образом чтят законодательство, обеспечивается уважительное отношение в области прав человека, обеспечивается многоуровневая защита персональных данных на самом высоком уровне.

4. Жалоба в ЕСПЧ дело «Владимира Николаевича Федорова против РФ» (Vladimir Nikolayevich Fedorov v. Russia) №48974/09, от 30.05.2017г

Суть дела: заявитель, бывший заведующий кафедрой фармакологии в Ярославской государственной медицинской академии, был задержан по подозрению в получении взяток, и ему была избрана мера пресечения в виде заключения под стражу. Заявитель жаловался на то, что избранная ему мера пресечения являлась чрезмерно жесткой и что ее продление не было оправдано с учетом материалов дела. Заявитель также утверждал, что отказ в свидании с женой во время нахождения под стражей нарушал его право на уважение семейной жизни.

Решение Европейского Суда по правам человека: Европейский Суд единогласно постановил, что в данном деле власти Российской Федерации не допустили нарушения требования пункта 3 статьи 5 Конвенции (право на свободу и личную неприкосновенность), но нарушили требования статьи 8 Конвенции (право на уважение частной и семейной жизни).

Из приведенных выше примеров, стоит отметить несколько моментов, имеющих важное значение: есть слабые стороны в информационной системе защиты данных, особенно в медицинском направлении. Есть механизм

защищающий права личности, то есть на законодательном уровне система разработала все рычаги воздействия на защиту конфиденциальных данных.

Страдает уровень разработки защиты на доступ к информации правообладателя.

Следует сделать вывод, что в нашей стране еще нет устойчивого фундамента по защите конфиденциальности, принято много законов и с каждым разом совершенствуются меры для соблюдения законодательства, но в области контроля за соблюдением исполнения требований не достаточно принятых мер, необходимо ужесточать систему наказания, как в виде штрафных санкций, так и в виде ужесточения ответственности.

2.2. СРАВНИТЕЛЬНЫЙ АНАЛИЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ В МЕЖДУНАРОДНОМ И РОССИЙСКОМ ПРАВЕ

Так уж сложились мнения, что по вопросам защиты личных данных от кибер- атак, существуют два подхода. Один из нах касается США и их единомышленников, второй России и сторонников данного подхода.

В первом случае имеется ввиду ужесточенные меры, призывающие к военным действиям, во втором мирное регулирование, поскольку военные действия не дают никаких гарантий, что применяя ужесточенный метод, не будут использоваться информационные ресурсы.

Стоит также обратить внимание, вернее не обойти значение, к 75 сессии в ООН, где Россия выдвинула создание группы, по решению данных проблем, где должны рассматривать нормы, представленные в резолюции и разработаны дополнительные поправки в них.

Созданной группой должны быть продолжены исследования в области защиты информационной безопасности, которые должны учитывать интересы и исследования научных сообществ, вопросы, относящиеся к бизнесу и прочие.

Сторонники первой группы же, в свою очередь настаивают на географическом распределении групп, где должны быть упоминания национальных вопросов регулирования международной безопасности, а также выдвинули уже действующие соглашения.

По различным источникам можно найти информацию, что российские данные постоянно подвергаются атакам со стороны, на что на протяжении двадцати лет, разработаны колоссальные системы защиты, но стоит отметь преимущество в компьютезированности со стороны американского государства.

Но, если говорить о нормативно-правовых актах, то в Российском законодательстве, в отличие от американского законодательства, есть законодательная база направленная на защиту биометрических данных и личной информации, а также существуют требования, закрепленные в постановлении.

В Европе уже более двух лет действует Общий регламент по защите персональных данных Европейского союза. Он дает гражданам право распоряжаться своими персональными данными, а также запрещает операторам передавать их третьим лицам.

На регламент ориентируются в США и Канаде. Россия также обновляет свое законодательство о персональных данных, в частности в Госдуму внесен законопроект, согласно которому вводится запрет на использование данных компаниями без согласия пользователя.

Имеется закон, в котором говорится об ответственности за недобросовестную рекламу, но как показывает практика мы все равно получаем нежелательные письма и звонки.

Юрист Журавлев предложил увеличить систему компенсации ущерба на каждого гражданина, в том числе с оператора.

С мнением юриста Журавлева, отчасти я согласна, и в его интервью для «газета.ру», он обозначил острую проблему угрозе персональным данным в условиях пандемии. Судя по тому, что происходит на данный момент, система была не готова к глобальной нагрузке и домашние сети подверглись к весомому испытанию.

Организация Объединенных Наций, МСЭ, УКГВ, УВКПЧ, ПРООН, ЮНЕП, ЮНЕСКО, УВКБ, ЮНИСЕФ, ЮНОПС, Добровольцы ООН, ООН-женщины, ВОЗ поддерживают принятие следующего совместного заявления в соответствии с Принципами ООН, касающимися защиты личных данных и неприкосновенности частной жизни, принятыми учреждениями системы ООН в поддержку использования данных и технологий в условиях борьбы с COVID-19 таким образом, чтобы обеспечивать уважение права на

неприкосновенность частной жизни и других прав человека и содействовать экономическому и социальному развитию.

Пандемия COVID-19 представляет собой глобальную чрезвычайную ситуацию, имеющую разрушительные последствия с точки зрения смерти людей и экономического спада и являющуюся значительным препятствием для продвижения к достижению Целей Организации Объединенных Наций в области устойчивого развития. Особую угрозу эта смертельно опасная болезнь и ее экономические последствия представляют для неимущих и уязвимых общин.

Все больше и больше фактических данных свидетельствуют о том, что сбор, использование, распространение и дальнейшая обработка данных могут способствовать ограничению распространения вируса и ускорению восстановления, особенно благодаря цифровому отслеживанию контактов. Так, например, данные о мобильности, получаемые благодаря тому, что люди используют мобильные телефоны, электронную почту, банковские операции, социальные сети и почтовые услуги, могут помочь в мониторинге распространения вируса и содействовать осуществлению деятельности, предусмотренной мандатами учреждений системы ООН [НКЦКИ, 4с].

Такой сбор и обработка данных, в том числе для цифрового отслеживания контактов и общего наблюдения за состоянием здоровья, могут включать в себя сбор огромного объема конфиденциальных персональных и неперсональных данных. Это может иметь значительные последствия после завершения начального этапа реагирования на кризис, в том числе в тех случаях, когда такие меры применяются в целях, не связанных непосредственно или конкретно с мерами реагирования на COVID-19, что может приводить к нарушению основных прав и свобод человека. Эта проблема приобретает особую актуальность, если некоторые чрезвычайные меры, введенные для борьбы с пандемией, такие как цифровое отслеживание контактов, становятся стандартной практикой.

Генеральный секретарь ООН в своей аналитической записке о правах человека и COVID-19 отметил, что «права человека имеют ключевое значение для разработки мер реагирования на пандемию как с точки зрения чрезвычайной ситуации в области общественного здравоохранения, так и в связи с более широким воздействием на жизнь людей и их средства к существованию. Права человека подразумевают, что центральное место отводится людям. Ответные меры, принимаемые в соответствии с правами человека и на основе их соблюдения, позволяют добиться лучших результатов в борьбе с пандемией, обеспечивая медицинскую помощь для всех и сохранение человеческого достоинства».

Любой сбор, использование и обработка данных учреждениями системы ООН в контексте пандемии COVID-19 должны основываться на правах человека и осуществляться с должным учетом применимых норм международного права и принципов защиты данных и неприкосновенности частной жизни, включая Принципы ООН, касающиеся защиты личных данных и неприкосновенности частной жизни. Любые меры, принимаемые в связи с пандемией COVID-19, должны также соответствовать мандатам соответствующих учреждений системы ООН и учитывать сбалансированность соответствующих прав, включая право на здоровье и жизнь и право на экономическое и социальное развитие.

С учетом Принципов ООН, касающихся защиты личных данных и неприкосновенности частной жизни, аналитической записки Генерального секретаря ООН о правах человека и COVID-19, а также соответствующих стандартов здравоохранения и гуманитарных норм сбор, использование и обработка данных учреждениями системы ООН в рамках их деятельности должны, как минимум: быть законными, ограниченными по охвату и времени, а также необходимыми и пропорциональными конкретным и обоснованным целям в борьбе с пандемией COVID-19; обеспечивать надлежащую конфиденциальность, безопасность, ограниченное по срокам хранение и надлежащее уничтожение или удаление данных в соответствии с

вышеупомянутыми целями; обеспечивать, чтобы любой обмен данными осуществлялся в соответствии с применимыми нормами международного права и принципами защиты данных и неприкосновенности частной жизни и анализировался на основе должной осмотрительности и оценки рисков; регулироваться любыми соответствующими механизмами и процедурами для обеспечения того, чтобы меры, принимаемые в отношении использования данных, были оправданы вышеупомянутыми принципами и целями и соответствовали им, и прекращаться, как только отпадет необходимость в таких мерах; и быть транспарентными в целях укрепления доверия к развертыванию как нынешних, так и будущих мероприятий.

Для того чтобы сдержать пандемию и свести к минимуму ее негативные последствия во всем мире, необходимо принимать скоординированные и всеобъемлющие глобальные меры реагирования в рамках всей ООН на основе солидарности. Несмотря на то, что это заявление направлено на решение проблем, связанных с нынешней пандемией COVID-19, оно может служить в качестве прецедента для использования данных в целях быстрого реагирования на любые будущие кризисы аналогичного масштаба на основе обеспечения защиты данных и неприкосновенности частной жизни.

Проблемы безопасности удаленного доступа во время новой пандемии определяются объективными и субъективными причинами. С одной стороны, стандартная домашняя точка доступа в Интернет менее сложна с точки зрения безопасности, с другой стороны, переход был неожиданным и резким.

В настоящее время существует множество отечественных решений в области информационной безопасности и международных рекомендаций по организации безопасного удаленного доступа. Мы кратко перечислим контрмеры в порядке подсистем безопасности: установление стабильной, предпочтительно многофакторной аутентификации; разграничение доступа к домашнему компьютеру (если это разрешено политикой безопасности организации); использование только защищенной корпоративной почты и доверенного облака; организация доверенного канала связи; наличие

антивируса, усиленного персональным брандмауэром; обеспечение режима шифрования на диске (в случае физической потери); контроль внешних носителей; наличие лицензионного программного обеспечения, обеспечивающего обновление и мониторинг наличия уязвимостей в системе; контроль физического доступа и безопасности; наличие системы резервного копирования и восстановления; использование гарантированного стирания информации и др. Самое главное- обучать и информировать пользователей об угрозах и контрмерах в процессе удаленной работы, особенно во время рабочих видеоконференций.

Что касается корпоративной сети, допускающей удаленную работу, то усовершенствования информационной безопасности имеют более систематическую форму, затрагивая технический сегмент, решая организационные вопросы (внедрение подсистемы управления безопасной удаленной работой, безопасное управление временем и т.д.), Обучение сотрудников и мониторинг их поведения. Эти вопросы хорошо освещены в литературе и на интернет- ресурсах.

Во время вспышки новой короновирусной инфекции весь ИТ-мир столкнулся с уникальной проблемой в области информационной безопасности, и учет опыта защищенной работы в компьютерных сетях во время пандемии неоценим в организационном и техническом плане.

К примеру, когда большая часть населения находилась в режиме самоизоляции, дети учились дистанционно, родители работали со своими рабочими базами данных, домашние сети подверглись кибер-атакам.

Новостные ленты пестрили видео с уроков в режиме онлайн, где нарушался режим проведения, а именно вторгались в идущий урок или лекцию, и всячески участвовали посторонние лица чтобы прервать данное занятие.

На международном уровне защита информации представлена как в кодексах в реальной жизни, так и в сети, и имеет одинаковую силу и наказание за нарушение.

Всемирная организация здравоохранения 19 сентября 2020 года сделала по этому поводу заявление, в котором рассмотрели вопросы защиты персональных данных.

Проблемы безопасности удаленного доступа во время новой пандемии коронавируса определяются «объективными и субъективными причинами.

Из исторического анализа, мы видим, что безопасность доступа на международном уровне более системно и имеет более высокие средства защиты. Так как нагрузка на глобальные сети в нашей стране произошла стремительно и система не была готова полностью, то у нас, с учетом рекомендаций более опытных «коллег», были разработаны некие рекомендации и найдены пути решений данной проблемы.

К таким мерам можно отнести, увеличение ряда шагов для прохождения системы опознавания и подтверждения личности, для работы из дома разграничить домашнюю сеть, увеличить систему защиты электронной почты и хранилища данных, рекомендовано использовать только лицензированные программные обеспечения и обязательное присутствие надежной антивирусной системы, также рекомендуется проводить периодическое обучение персонала по ИБ.

Следует сделать вывод, по данному анализу. На международном уровне, так же как в российском праве законодательная база достаточно регулируемая по вопросам информационной безопасности. Разница лишь на уровне контроля, так как на международном уровне принятые решения строго контролируются и жестко наказывают за нарушение и/или неисполнение, а в российском законодательстве действуют смягчающие меры и не высокие штрафные санкции. В ходе анализа правового регулирования в Российской Федерации, необходимо внести изменения или дополнения в ФЗ от 27.07.2006г N 149-ФЗ(ред. От 08.06.2020г) «Об информации, информационных технологиях и защите информации», а именно зафиксировать ответственность банка и возмещение причиненного ущерба, и дополнить ответственность провайдеров, назначить ответственное

лицо, которое будет нести ответственность за просмотр личных данных незарегистрированным пользователям

ЗАКЛЮЧЕНИЕ

В процессе изучения вопросов информационной безопасности личности, учитывая цели исследования, следует подвести итоги и остановиться на основных выводах.

1. Если говорить по историческим аспектам, то следует сделать вывод, что неотъемлемо растет развитие общества в области информационных технологий, и направленность государства на решение конфликтных ситуаций в информационном потоке, прилагает максимум усилий для недопущения вмешательства сторонних в частную жизнь и государственные вопросы. Но следует учесть, что при развитии технологического прогресса в области информационной технологии, также развивается и преступный фактор, и порой с изобретением новых программ, казалось для упрощения оформления тех же заказов товаров или услуг, образуются слабые стороны в алгоритме, что предоставляет потенциальный доступ к информации. На различных этапах развития технологий, следует вносить поправки в законодательство и учитывать риски возникновения конфликтных ситуаций.

К примеру, все новые проекты с использованием ИКТ, должны проходить регистрацию и получать разрешение на вид деятельности, соответственно, должны приобретать лицензии и программное обеспечение по защите данных, и прочие схемы действий для возможности существования на информационной платформе. Я считаю, что принцип работы с данными и защита их, должна иметь единый международный стандарт, так как в той или иной степени торговые отношения сейчас действуют для всех, соответственно и работать должны по единому стандарту, и метод контроля должен быть разработан в едином стандарте.

2. Понятие «международная защита информационной безопасности» подверглось различной интерпретации, с 1983 года в него входили межгосударственные отношения, не противоречащие глобальным интересам в области информации, которые закреплены в международном

праве. С развитием информационных технологий, в данное понятие вкладывали обширное значение, но одно могу сказать, что четкого определения «международная защита информационной безопасности» отсутствует и весомые аргументы приведены выше.

Можно сделать заключение и дать определение, что входит в данный смысл выражения «международная защита информационной безопасности личности»- это совокупность систем и процедур различных международных органов, в чьих интересах на первом плане идет защита личных данных, «международных стандартов в защите прав человека», разработка единого механизма соблюдения контроля за выполнением стандартов государствами.

3. Следует сделать вывод, что в нашей стране еще нет устойчивого фундамента по защите конфиденциальности, принято много законов и с каждым разом совершенствуются меры для соблюдения законодательства, но в области контроля за соблюдением исполнения требований не достаточно принятых мер, необходимо ужесточать систему наказания, как в виде штрафных санкций, так и в виде ужесточения ответственности. То есть, на законодательном уровне применяются все меры обеспечения защиты прав в области информационной безопасности, а как показывает практика, нет жесткого регулирования контроля исполнительности законодательства.

Рассматривая высказывания различных ученых, изучая информацию с форумов, изучая статьи, разбираясь в законодательных проектах, могу сказать с твердой уверенностью, что защита информационных данных более развита в международной практике, поскольку в зарубежных странах частные лица ранее начали осваивать просторы интернета в своих интересах, далее пошли рыночные и платежные системы, и соответственно ранее столкнулись с использованием личных данных, далеко не в благих целях.

Необходимо вести обязательную регистрацию IP-адреса, возможно даже через определенное программное обеспечение, где каждый адрес, как паспортные данные, должен проходить многоуровневую защиту и

идентификацию, и при любой спорной ситуации, правоохранительный орган мог получить данные правообладателя.

Регистрация такого адреса должна производиться в момент закупа телефона, компьютерной системы и/или подводя интернет к объекту. При продаже или утери объекта движимого или недвижимого имущества, привязанного к адресу, необходима перерегистрация в определенной системе.

Утечка персональных данных может произойти практически из любой организации. Однако в серьезных, богатых, длительное время существующих организациях такая вероятность меньше, а возможностей исправления ее последствий - больше.

Поэтому первая рекомендация - не передавайте персональные данные в организации, в которых вы не уверены. Прежде всего речь идет о неизвестных вам интернет-магазинах и интернет-сайтах.

Вторая рекомендация - никогда не пересылайте фотографии, копии своих паспортов, банковских карт неизвестным вам лицам и тем, в ком вы недостаточно уверены.

Третья рекомендация - при пересылке личных данных в знакомые вам организации пользуйтесь официальными ящиками электронной почты, указанными на официальном сайте.

Четвертая рекомендация - фиксируйте в специальном списке все созданные вами аккаунты в социальных сетях, личные кабинеты, сайты, на которых вы регистрировались. Периодически проводите ревизию этого списка. Закрывайте все аккаунты, кабинеты, регистрации и т.п., которыми вы не пользуетесь.

Пятая рекомендация - при посещении организаций, где при входе требуют предъявлять паспорт и фиксируют паспортные данные, старайтесь паспорт показывать, но не передавать работникам службы охраны в руки. Желательно, чтобы вы сами заполняли формуляры со своими паспортными данными.

Если каждый будет под жестким контролем, то, как мне кажется, чтобы совершить то или иное действие относящиеся или имеющие отношение к нарушению законодательства, правообладатель лишний раз подумает, стоит ли оно того.

Соответственно даже среди населения выработались тенденции, на которые стоит обращать внимания, дабы не стать жертвой интернет-мошенников. Плюс ко всему нам стоит обратить внимание на зарубежную судебную практику по защите частной информации и принять во внимание, что на законодательном уровне международная система ужесточенная в плане контроля и соблюдения законов.

4. На международном уровне, так же как в российском праве законодательная база достаточно регулируемая по вопросам информационной безопасности. Разница лишь на уровне контроля, так как на международном уровне принятые решения строго контролируются и жестко наказывают за нарушение и/или неисполнение, а в российском законодательстве действуют смягчающие меры и не высокие штрафные санкции.

В ходе анализа правового регулирования в Российской Федерации, необходимо внести изменения или дополнения в ФЗ от 27.07.2006г N 149-ФЗ(ред. От 08.06.2020г) «Об информации, информационных технологиях и защите информации», а именно зафиксировать ответственность банка и возмещение причиненного ущерба в статью 14.1, и дополнить ответственность провайдеров, назначить конкретное лицо, к примеру директор компании, которое будет нести ответственность за просмотр личных данных, таких даже, как номер телефона, незарегистрированным пользователям в статью 17.

В российском законодательстве стоит ужесточить меры наказания за использование чужих данных в любых целях, без разрешения на то, и за нарушение законов применять более серьезные меры, как в увеличении штрафных санкций, так и уголовное наказание.

Данная тема до конца не изучена и нет конкретных мероприятий по устранению проблем информационной безопасности. С каждым днем при разработке системы для охраны персональных данных, в виду неотъемлемого прогресса развития информационных технологий, найдутся пробелы или по другому «лазейки», слабые места. Эта тема нуждается в изучении и исследовании с каждым цифровым и техническим прогрессом.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Нормативные правовые акты

1. Конституция Российской Федерации. Принята всенародным голосованием 12 декабря 1993 г. с изм. от 1 июля 2020 г. // Собрание законодательства РФ. – 2020. - № 31. – ст. 4398.

2. Гражданский процессуальный кодекс Российской Федерации: от 14 ноября 2002 г.: по состоянию на 31.07.2020 г. // Собрание законодательства Российской Федерации. – 2002. – № 46. – Ст. 4531.

3. Конвенция об обеспечении международной информационной безопасности(Концепция)/ Утверждена 22.09.2011/-2011.-ст.7

4. Международный договор/ Соглашение от 25 декабря 2013 года/ соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности// URL:http://docs.cntd.ru/document/499074140 (дата обращения: 26.10.2020г)

5. Европейская конвенция о защите физических лиц в вопросах, касающихся автоматической обработки личных данных/ принятая Советом Европы в 1985 году// URL: http://www.consultant.ru/document/ cons_do c_LAW_121499/(дата обращения: 24.10.2020г)

6. Резолюция Европейского парламента 1979 года «О защите прав личности в связи с прогрессом информатизации» //URL: https://nisse.ru/articles/details.php?ELEMENT_ID=98127/ (дата обращения: 21.10.2020г)

7. «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года» /утв. Президентом РФ 24.07.2013 № Пр-1753// URL:https://www.garant.ru/products/ipo/prime/doc/70541072/ (Дата обращения: 27.10.2020г)

8. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» URL:https://www.garant.ru/products/ipo/prime/doc/71456224/ (дата обращения: 01.11.2020г)

9. Национальный стандарт РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006)/утв. Приказом Федерального агентства по техническому регулированию и метрологии от 27.12.2006г)- N373-ст// URL:https://base.garant.ru/193664/ (дата обращения: 16.10.2020г)

10. Указ Президента РФ «Об утверждении Доктрины информационной безопасности Российской Федерации» от 05.12.2016- N 646// URL: https://base.garant.ru/71556224/ (Дата обращения: 20.10.2020г)

Научная и учебная литература

1. Алексеев Г.В., Кириленко В.П. «Международное право и информационная безопасность государств» -СПб- 2016- ст 396

2. Баринов С.В. «О правовом определении понятия «Информационная безопасность личности» / «Актуальные проблемы российского права»/-2016-N4(65)-ст 9

3. Бармен Скотт. Разработка правил информационной безопасности. М.: Вильямс-2002г-ст 208

4. Бачило И.Л. Эффективность законодательства в области обеспечения информационной безопасности.// ВИНИТИ РАН. Научно – техническая информация. Серия 1. М., 199б- N7

5. Галатенко, В.А. Стандарты информационной безопасности./ М. Интернет-университет информационных технологий- 2010-с326/ ISBN 5-9556-0007-8

6. Галицкий, А.В., Защита информации в сети / Анализ технологий и синтез решений. Рябко С.Д., Шаньгин В.Ф/ М.: ДМК Пресс- 2011г-ст 26

7. Герасименко В.А., Малюк А.А. Основы защиты информации. М.- 1997. — 537 с. — ISBN: 5-88852-010-1

8. Доктрина информационной безопасности (проект) МВК СБ РФ. М.-2016г//URL: https://tass.ru/info/3845810 (Дата обращения: 19.10.2020г)

9. Кара- Мурза С. Г. Манипуляция сознанием. (Серия: История России. Современный взгляд). Москва-2000-ст 480

10. Кашанина Т.В., Кашанин А.В. Основы российского права./ Учебник. Москва, -1997г-ст 368

11. Концепция информационной безопасности Российской Федерации (проект).// Информационный сборник «Безопасность»-1995г-N1-ст 28

12. Концепция развития безопасности информационных технологий: обеспечение защиты информации в проектах информатизации России.- Москва- 1992-ст 26

13. Каймин В.А.. Информатика. /Учебное пособие. 2-ое изд./ М.РИОР -2007-129с. //ISBN 5- 36900179-0

14. Лепехин А. Н. Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты. М.: Тесей- 2008-ст 176

15. Лопатин В.Н. Информационная безопасность России./ Москва- 2003- ст 433

16. Мовчан А. П. Международный правопорядок / РАН. Ин-т государства и права. – М. , 1996. – 102 с

17. Об угрозах безопасности информации, связанных с пандемией коронавируса (COVID-19.). НКЦКИ, 2020. – ALRT-20200320.1 (20 марта 2020 г.) – ст 4

18. Первый Фонд «Общественное мнение»/ Опросы «Интернет в России / Россия в Интернете»/ Выпуск 14- 2005-ст36 .

19. Правила поведения в области обеспечения международной информационной безопасности: письмо постоянных представителей Казахстана, Киргизии, Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 12 сентября 2011 г.

На имя Генерального секретаря. A/66/359 // URL: https://www.rus.rusemb.org.uk/data/doc/internationalcoderus.pdf (Дата обращения: 19.10.2020г)

20. Первый комитет Генеральной Ассамблеи ООН «кибертерроризм: угроза национальной и международной безопасности»/ Доклад Эксперта/ Тверь 2018г// URL: https://docplayer.ru/84342686-Pervyy-komitet-generalnoy-assamblei-oon-kiberterrorizm-ugroza-nacionalnoy-i-mezhdunarodnoy-bezopasnosti-doklad-eksperta.html/ (Дата обращения: 19.10.2020г)

21. Первый Фонд «Общественное мнение». Опросы «Интернет в России / Россия в Интернете». Выпуск 14. 2005

22. Павлова Л.В. «Международная защита прав человека и ее эволюция на современном этапе»/ Белорусский журнал международного права и международных отношений- 1996- N1- ст 24

23. Рекомендации по обеспечению безопасности объектов критической информационной инфраструктуры при реализации дистанционного режима исполнения должностных обязанностей работниками субъектов критической информационной инфраструктуры. ФСТЭК России, 2020. – Письмо ФСТЭК России от 20 марта 2020 г. N 240/84/389 – с 3

24. Стивен Леви ХАКЕРЫ, Герои Компьютерной Революции = Hackers, Heroes of the computer revolution. — «A Penguin Book Technology», 2002. — С. 337.

25. Скородумова О. Б. Хакеры // Знание. Понимание. Умение. — 2005. — № 4. — С. 159- 161.

26. Стивен Леви ХАКЕРЫ, Герои Компьютерной Революции = Hackers, Heroes of the computer revolution. — «A Penguin Book Technology»- 2002- 337с

27. Скородумова О. Б. «Хакеры» // Знание. Понимание. Умение. — 2005-N 4- ст 161

28. Фролов К.В. «Безопасность России: правовые, социально- экономические и национально- технические аспекты. Словарь терминов и определений»/ М., -1999- ст 56

29. Цыгичко В.Н., Смолян Г.Л., Черешкин Д.С. Информационное оружие как геополитический фактор и инструмент силовой политики.-Москва- 2005

30. Черниченко С.В. «Личность и международное право»/М., 1974, Указ.соч. 168с

31. Шаньгин, В.Ф. Защита компьютерной информации/Эффективные методы и средства. М.: ДМК Пресс-2010-ст 78

32. Юсупов Р.М. Информационная безопасность /основа национальной безопасности.- Санкт-Петербургский институт информатики и информатизации РАН- СПб.- 2007

33. Ярочкин, В.И. Информационная безопасность. Учебник для вузов. Фонд « Мир»/Акад. Проект/- 2010-ст 639

Материалы практики

1. Постановление ЕСПЧ от 28 мая 2019 года по делу «Сидорова (Sidorova) против Российской Федерации» (жалоба N 35722/15).

2. Дело «Авилкина и другие» против Российской Федерации» (Жалоба N 1585/09) Постановление Суда Страсбург, 6 июня 2013 г.

3. Дело «Schrems II» 16 июля 2020 г. Суд Европейского союза (CJEU) (Дело N C-311/18)

4. Жалоба в ЕСПЧ дело «Владимира Николаевича Федорова против РФ» (Vladimir Nikolayevich Fedorov v. Russia) №48974/09, от 30.05.2017г