ЛЕКЦИЯ «БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И ЕЕ ПРАВОВОЕ ОБЕСПЕЧЕНИЕ, КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ»

ВОПРОСЫ ЛЕКЦИИ:

1. Проблема информационной безопасности общества.
2. Задачи информационной безопасности общества.
3. Нормативно-правовые основы информационной безопасности в РФ.
4. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации.

ЛИТЕРАТУРА:

1. Бабаш А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.

2. Бирюков А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013. - 474 с.

3. Федотова Е.Л. Информационные технологии и системы: Учебное пособие. - М.: ИД. "Форум" : ИНФРА - М. 2013.- 352 с.

1. Проблема информационной безопасности общества

Информационная безопасность является одной из проблем, с которой столкнулось современное общество в процессе массового использования автоматизированных средств ее обработки.

Проблема информационной безопасности обусловлена возрастающей ролью информации в общественной жизни. Современное общество все более приобретает черты информационного общества.

Наряду с понятием информационная безопасность часто используют еще несколько понятий.

Информационная война - информационное противоборство с целью нанесения ущерба важнейшим структурам противника, подрыва его политической и социальной систем, а также дестабилизации общества и государства противника.

Информационная преступность - проведение информационных воздействий на информационное пространство субъекта в противоправных целях.

С понятием "информационная безопасность" в различных контекстах связаны различные определения. Так, в Законе РФ "Об участии в международном информационном обмене" информационная безопасность определяется как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства. Подобное же определение дается и в Доктрине информационной безопасности Российской Федерации, где указывается, что информационная безопасность характеризует состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

Оба эти определения рассматривают информационная безопасность в национальных масштабах и поэтому имеют очень широкое понятие.

Наряду с этим характерно, что применительно к различным сферам деятельности так или иначе связанным с информацией понятие "информационная безопасность" принимает более конкретные очертания. Так, например, в "Концепции информационной безопасности сетей связи общего пользования Российской Федерации" даны два определения этого понятия.

1. Информационная безопасность – это свойство сетей связи общего пользования противостоять возможности реализации нарушителем угрозы информационной безопасности.

2. Информационная безопасность – свойство сетей связи общего пользования сохранять неизменными характеристики информационной безопасности в условиях возможных воздействий нарушителя.

Необходимо иметь в виду, что при рассмотрении проблемы информационной безопасности нарушитель необязательно является злоумышленником. Нарушителем информационной безопасности может быть сотрудник, нарушивший режим информационной безопасности или внешняя среда, например, высокая температура, может привести к сбоям в работе технических средств хранения информации и т. д.

Сформулируем следующее определение "информационной безопасности".

Информационная безопасность – это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.

Что включает информационная безопасность:

- Состояние защищенности информационного пространства, как государства, так и конкретного человека.
- Состояние информации, при котором исключается или сильно затрудняется нарушение таких свойств, как конфиденциальность, доступность, целостность.
- Состояние инфраструктуры, при котором информация используется строго по назначению и не оказывает негативного воздействия на систему при ее использовании.
- Финансовую составляющую (базы данных банков, системы электронных платежей и т.д.).

Понятие информационной безопасности в узком смысле этого слова подразумевает:

- сохранность необходимых данных;
- надежность работы компьютера;

- защиту информации от внесения в нее изменений неуполномоченными лицами;
- защиту электронного документооборота и информации передающейся по сети интернет.

Рассматривая информацию как товар можно сказать, что нанесение ущерба информации в целом приводит к материальным затратам. Например, раскрытие технологии изготовления оригинального продукта приведет к появлению аналогичного продукта, но от другого производителя, и, как следствие, владелец технологии, а может быть и автор, потеряют часть рынка и т. д.

С другой стороны, рассматривая информацию как субъект управления (технология производства, расписание движения транспорта и т. д.), можно утверждать, что изменение ее может привести к катастрофическим последствиям в объекте управления – производстве, транспорте и др.

Именно поэтому при определении понятия "информационная безопасность" на первое место ставится защита информации от различных воздействий.

Поэтому под защитой информации понимается комплекс мероприятий, направленных на обеспечение информационной безопасности.

Согласно ГОСТу 350922-96 защита информации - это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Решение проблемы информационной безопасности, как правило, начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем. Это обусловлено тем, что для разных категорий субъектов характер решаемых задач может существенно различаться. Например, задачи решаемые администратором локальной сети по обеспечению информационной безопасности, в значительной степени отличаются от задач, решаемых пользователем на домашнем компьютере, не связанном сетью.

Исходя из этого, отметим следующие **важные выводы**:

- задачи по обеспечению информационной безопасности для разных категорий субъектов могут существенно различаться;
- информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации – это принципиально более широкое понятие.

При анализе проблематики, связанной с информационной безопасностью, необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что информационная безопасность есть составная часть информационных технологий – области, развивающейся беспрецедентно высокими темпами. В области информационной безопасности важны не столько отдельные решения (законы, учебные курсы, программно-технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие, как минимум, адекватно реагировать на угрозы информационной безопасности или предвидеть новые угрозы и уметь им противостоять.

В ряде случаев понятие "информационная безопасность" подменяется термином "компьютерная безопасность". В этом случае информационная безопасность рассматривается очень узко, поскольку компьютеры только одна из составляющих информационных систем. Несмотря на это, в рамках изучаемого курса основное внимание будет уделяться изучению вопросов, связанных с обеспечением режима информационной безопасности применительно к вычислительным системам, в которых информация хранится, обрабатывается и передается с помощью компьютеров.

Согласно определению, компьютерная безопасность зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электроснабжения, жизнеобеспечения, вентиляции, средства коммуникаций, а также обслуживающий персонал.

Доступность информации

Как уже отмечено ранее, информационная безопасность – многогранная область деятельности, в которой успех может принести только систематический, комплексный подход.

Обеспечение информационной безопасности в большинстве случаев связано с комплексным решением трех задач:

1. Обеспечением доступности информации.
2. Обеспечением целостности информации.
3. Обеспечением конфиденциальности информации.

Именно доступность, целостность и конфиденциальность являются равнозначными составляющими информационной безопасности.

Информационные системы создаются для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, то это, очевидно, наносит ущерб всем пользователям.

Роль доступности информации особенно проявляется в разного рода системах управления – производством, транспортом и т. п. Менее драматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей, например, продажа железнодорожных и авиабилетов, банковские услуги, доступ в информационную сеть Интернет и т. п.

Доступность – это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.

Фактор времени в определении доступности информации в ряде случаев является очень важным, поскольку некоторые виды информации и информационных услуг имеют смысл только в определенный промежуток времени. Например, получение заранее заказанного билета на самолет после его вылета теряет всякий смысл. Точно так же получение прогноза погоды на вчерашний день не имеет никакого смысла, поскольку это событие уже наступило. В этом контексте весьма уместной является поговорка: "Дорога ложка к обеду".

Целостность информации

Целостность информации условно подразделяется на статическую и динамическую. **Статическая** целостность информации предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации. **Динамическая** целостность информации включает вопросы корректного выполнения сложных действий с информационными потоками, например, анализ потока сообщений для выявления некорректных, контроль правильности передачи сообщений, подтверждение отдельных сообщений и др.

Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, например техническими, социальными и т. д.

Так, ошибка в управляющей программе приведет к остановке управляемой системы, неправильная трактовка закона может привести к его нарушениям, точно также неточный перевод инструкции по применению лекарственного препарата может нанести вред здоровью. Все эти примеры иллюстрируют нарушение целостности информации, что может привести к катастрофическим последствиям. Именно поэтому целостность информации выделяется в качестве одной из базовых составляющих информационной безопасности.

Целостность – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений.

Конфиденциальность информации

Конфиденциальность – самый проработанный у нас в стране аспект информационной безопасности. К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем в России связана с серьезными трудностями. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного

средства обеспечения конфиденциальности стоят многочисленные законодательные и технические проблемы.

Конфиденциальная информация есть практически во всех организациях. Это может быть технология производства, программный продукт, анкетные данные сотрудников и др. Применительно к вычислительным системам в обязательном порядке конфиденциальными данными являются пароли для доступа к системе.

Конфиденциальность – гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена.

Нарушение каждой из трех категорий приводит к нарушению информационной безопасности в целом. Так, нарушение доступности приводит к отказу в доступе к информации, нарушение целостности приводит к фальсификации информации и, наконец, нарушение конфиденциальности приводит к раскрытию информации.

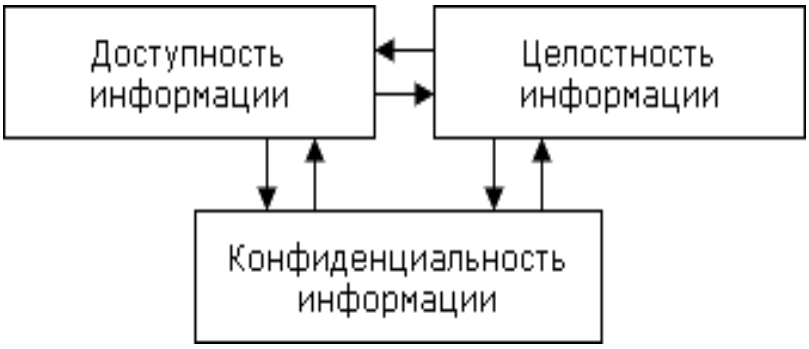

Рисунок 1. Составляющие информационной безопасности

Как уже отмечалось, выделение этих категорий в качестве базовых составляющих информационной безопасности обусловлено необходимостью реализации комплексного подхода при обеспечении режима информационной безопасности. Кроме этого, нарушение одной из этих категорий может привести к нарушению или полной бесполезности двух других. Например, хищение пароля для доступа к компьютеру (нарушение конфиденциальности) может привести к его блокировке, уничтожению данных (нарушение доступности

информации) или фальсификации информации, содержащейся в памяти компьютера (нарушение целостности информации).

2. Задачи информационной безопасности общества

Анализ основ информационной безопасности показал, что обеспечение безопасности является задачей комплексной. С одной стороны режима информационной, информационная безопасность предполагает, как минимум, обеспечение трех ее составляющих - доступность, целостность и конфиденциальность данных. И уже с учетом этого проблему информационной безопасности следует рассматривать комплексно. С другой стороны, информацией и информационными системами в буквальном смысле "пронизаны" все сферы общественной деятельности и влияние информации на общество все нарастает, поэтому обеспечение информационной безопасности также требует комплексного подхода.

В этой связи вполне закономерным является рассмотрение проблемы обеспечения информационной безопасности на нескольких уровнях, которые в совокупности обеспечивали бы защиту информации и информационных систем от вредных воздействий, наносящих ущерб субъектам информационных отношений.

Рассматривая проблему информационной безопасности в широком смысле, можно отметить, что в этом случае речь идет об информационной безопасности всего общества и его жизнедеятельности, при этом на информационную безопасность возлагается задача по минимизации всех отрицательных последствий от всеобщей информатизации и содействия развитию всего общества при использовании информации как ресурса его развития.

В этой связи основными задачами информационной безопасности в широком смысле являются:

- защита государственной тайны, т.е. секретной и другой конфиденциальной информации, являющейся собственностью государства, от всех видов несанкционированного доступа, манипулирования и уничтожения;
- защита прав граждан на владение, распоряжение и управление принадлежащей им информацией;
- защита прав предпринимателей при осуществлении ими коммерческой деятельности;
- защита конституционных прав граждан на тайну переписки, переговоров, личную тайну.

Рассматривая проблему информационной безопасности в узком смысле, отметим, что в этом случае речь идет о совокупности методов и средств защиты информации и ее материальных носителей, направленных на обеспечение целостности, конфиденциальности и доступности информации.

Исходя из этого, выделим следующие задачи информационной безопасности:

- защита технических и программных средств информатизации от ошибочных действий персонала и техногенных воздействий, а также стихийных бедствий;
- защита технических и программных средств информатизации от преднамеренных воздействий.

Заметим, что понятие "компьютерная безопасность", которому посвящена большая часть данного курса, как раз подходит под определение информационной безопасности в узком смысле, но не является полным ее содержанием, поскольку информационные системы и материальные носители информации связаны не только с компьютерами.

Уровни формирования режима информационной безопасности

С учетом изложенного выделим три уровня формирования режима информационной безопасности:

- законодательно-правовой;
- административный (организационный);

- программно-технический.

Законодательно-правовой уровень включает комплекс законодательных и иных правовых актов, устанавливающих правовой статус субъектов информационных отношений, субъектов и объектов защиты, методы, формы и способы защиты, их правовой статус. Кроме того, к этому уровню относятся стандарты и спецификации в области информационной безопасности. Система законодательных актов и разработанных на их базе нормативных и организационно-распорядительных документов должна обеспечивать организацию эффективного надзора за их исполнением со стороны правоохранительных органов и реализацию мер судебной защиты и ответственности субъектов информационных отношений. К этому уровню можно отнести и морально-этические нормы поведения, которые сложились традиционно или складываются по мере распространения вычислительных средств в обществе. Морально-этические нормы могут быть регламентированными в законодательном порядке, т. е. в виде свода правил и предписаний. Наиболее характерным примером таких норм является Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ США. Тем не менее, эти нормы большей частью не являются обязательными, как законодательные меры.

Административный уровень включает комплекс взаимокоординируемых мероприятий и технических мер, реализующих практические механизмы защиты в процессе создания и эксплуатации систем защиты информации. Организационный уровень должен охватывать все структурные элементы систем обработки данных на всех этапах их жизненного цикла: строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и проверки, эксплуатация.

Программно-технический уровень включает три подуровня: физический, технический (аппаратный) и программный. Физический подуровень решает задачи с ограничением физического доступа к информации и информационным системам, соответственно к нему относятся технические средства, реализуемые

в виде автономных устройств и систем, не связанных с обработкой, хранением и передачей информации: система охранной сигнализации, система наблюдения, средства физического воспрепятствования доступу (замки, ограждения, решетки и т. д.).

Средства защиты аппаратного и программного подуровней непосредственно связаны с системой обработки информации. Эти средства либо встроены в аппаратные средства обработки, либо сопряжены с ними по стандартному интерфейсу. К аппаратным средствам относятся схемы контроля информации по четности, схемы доступа по ключу и т. д. К программным средствам защиты, образующим программный подуровень, относятся специальное программное обеспечение, используемое для защиты информации, например антивирусный пакет и т. д. Программы защиты могут быть как отдельные, так и встроенные. Так, шифрование данных можно выполнить встроенной в операционную систему файловой шифрующей системой EFS (Windows 2000, XP) или специальной программой шифрования.

Подчеркнем, что формирование режима информационной безопасности является сложной системной задачей, решение которой в разных странах отличается по содержанию и зависит от таких факторов, как научный потенциал страны, степень внедрения средств информатизации в жизнь общества и экономику, развитие производственной базы, общей культуры общества и, наконец, традиций и норм поведения.

3. Нормативно-правовые основы информационной безопасности в РФ

Становление государственной информационной политики в России началось в конце двадцатого века, когда правительство осознало необходимость адаптации общества к стремительным преобразованиям в экономической жизни и к потребностям нового «информационного общества», которое в России только начинало формироваться. Первым проектом законодательного акта, регулирующего информационную активность была концепция информатизации

общества, разработанная в 1989 году и одобренная соответствующим комитетом Верховного Совета СССР. На основе данной концепции были подготовлены проекты общесоюзной программы информатизации и республиканской программы «Информатизация России» (1990-1991 гг.), но в силу политических и экономических причин данные программы так и не были приняты и не начали действовать.

Законодательная база в сфере информационной безопасности включает пакет Федеральных законов, Указов Президента РФ, постановлений Правительства РФ, межведомственных руководящих документов и стандартов. Не будем забывать и Конституцию Российской Федерации.

Первый закон, регулирующий отношения в области производства, обращения и распространения информации появился только в 1995 году с названием «Об информации, информатизации и защите информации» от 20.02.1995 N 24-ФЗ.

Данный закон был призван в новой России регулировать отношения, возникающие при: формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации; создании и использовании информационных технологий и средств их обеспечения; защите информации, прав субъектов, участвующих в информационных процессах и информатизации о чем указано в первой статье закона. Закон состоял из 5 глав и 25 статей и был на то время одним из самых прогрессивных нормативных правовых актов. Безусловным преимуществом данного закона является перечень терминов и определений, используемых в законе, что исключило разночтения в правоприменительной практике и способствовало единообразному применению закона в отношениях, им регулируемых, что выгодно его отличало от других нормативных актов того времени.

Со временем жизненные реалии потребовали модернизации нормативной базы и приведения ее в соответствие с потребностями возросшего

информационного обмена в обществе. Всего через 10 лет после принятия закона «Об информации..» 1995 года информационные отношения настолько изменились, что потребовалось принятие нового законодательного акта, устранившего новые правовые пробелы. Был принят новый закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», который с многочисленными изменениями и дополнениями действует по сей день. Новый закон не разделен на главы и изначально состоял из 18 статей. К сегодняшнему дню содержание данного закона насчитывает 36 статей, то есть, за 13 лет он увеличился в два раза.

Законы 1995 и 2006 годов регулируют одну и ту же сферу общественной жизни – отношения в сфере информации и называются практически одинаково, только в названии закона 1995 года указано «…информатизации..», что подчеркивает технологическую направленность правового акта, а в названии закона 2006 года указано «..информационных технологиях…» что расширяет сферу действия закона на все информационные технологии и, в то же время, конкретизирует его предмет. Несмотря на то, что с введением в действие закона 2006 года закон 1995 года утратил силу, многие исследователи находят в старом законе то, чего нет в новом и в чем состояло его преимущество. В то же время можно выделить множество преимуществ закона 2006 года перед старым.

Выделим достоинства и недостатки законов «Об информации..» 1995 года и 2006 года.

Закон «Об информации, информатизации и защите информации» от 20.02.1995 N 24-ФЗ имеет следующие достоинства:

- понятия «информация», «информационные ресурсы», «информационная система», «персональные данные» и другие получили законодательно закрепленное определение, что поставило защиту информации на новый уровень,

- закон впервые закрепил правовые основы информации,

- закон определил обязанности государственных органов в сфере информации,

- закон дал определение документа как материального носителя информации и определил документ как право собственности,

- закон установил правовой режим информационных ресурсов, информационных систем и технологий,

- закон установил требования к сбору и обработке персональных данных,

- закон установил правовой режим доступа к информации, ее предоставления.

В целом закон «Об информации…» 1995 года создал всеобъемлющую правовую базу сбора, хранения, распространения и использования информации. Вместе с тем, закон «Об информации…» 1995 года имел два существенных недостатка:

1. Не учитывалась международная практика регулирования информационных отношений. Как показало время, международный аспект информационных отношений чрезвычайно важен. С распространением сети интернет доступ к информационным ресурсам всего мира получил каждый пользователь из любой точки мира и вопрос международной защиты информации встал очень остро.

2. Содержание закона имело излишнюю технологичность. Законом регулировался как правовой режим информации, так и процессы информационного обеспечения, что зачастую вызывало противоречия.

Оба указанных недостатка закона «Об информации …» 1995 года были устранены в новом законе 2006 года № 149-Ф «Об информации, информационных технологиях и о защите информации».

Новый закон устранил многие пробелы и противоречия действующего российского законодательства в соответствии с международной практикой регулирования информационных отношений. Закон закрепил существование информации как самостоятельного объекта правовых отношений и установил, что его положения не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации.

В целом закон «Об информации …» 2006 года устанавливает более четкое правовое регулирование информационных отношений, учитывает международные особенности информационного обмена и устанавливает более четкие правовые гарантии защиты информации.

В качестве главного достоинства закона 2006 года стоит отметить определение информации как объекта гражданских прав, чего не было в законе 1995 года, где под объектом гражданских прав понималась информация, отраженная в документе, что вызывало трудности защиты персональных данных, информационных баз данных и других информационных объектов, не имеющих вещественной формы. Также, к безусловным достоинствам закона 2006 года относят его гибкость и способность учитывать современные информационные реалии с учетом соответствующих изменений. Так, в 2019 году в Государственную Думу РФ внесен Законопроект о цифровом профиле, который представляет собой поправки к законам «Об информации», «О персональных данных», «О связи» и «Об основах охраны здоровья граждан» в части уточнения процедур идентификации и аутентификации, он внесен в Госдуму 5 июля группой депутатов. Поправки предлагают свести воедино все имеющиеся в ведомствах данные о каждом гражданине на единой платформе.

Как пишется в статье «Цифровой профиль российского гражданина может стать удобной мишенью для хакеров», опубликованной 13 ноября 2019 года на IKSMEDIA.RU, - законопроект о создании цифровых профилей граждан России подвергся критике со стороны ФСБ. По ее мнению, обработка данных в рамках единой инфраструктуры значительно повысит риски утечек информации, в том числе о судьях, прокурорах, следователях и сотрудниках силовых ведомств. Как пишет «КоммерсантЪ», руководитель службы оперативной информации и международных связей ФСБ Сергей Беседа сообщил начальнику государственно-правового управления президента РФ Ларисе Брычевой, что законопроект не соотносится с принципами действующего закона «О персональных данных», поскольку «не содержит конкретных целей, для

достижения которых предусматривается обработка персональных данных в предлагаемом объеме».

Работа по созданию нормативной базы предусматривает разработку новых или корректировку существующих законов, положений, постановлений и инструкций, а также создание действенной системы контроля за исполнением указанных документов. Необходимо отметить, что такая работа в последнее время ведется практически непрерывно, поскольку сфера информационных технологий развивается стремительно, соответственно, появляются новые формы информационных отношений, существование которых должно быть определено законодательно.

В этой связи будет не лишним напомнить еще несколько важнейших документов своего времени: Концепцию национальной безопасности РФ, введенную указом Президента РФ №24 в январе 2000 г., Доктрину информационной безопасности Российской Федерации, утвержденную Президентом Российской Федерации 9 сентября 2000 г. Доктрина представляет собой свод официальных взглядов на обеспечение национальной безопасности государства в информационной сфере, под которой понимают совокупность информации, сайтов, сетей связи, а также государственных и частных компаний, обеспечивающих их работу.

Доктрина, как документ, охватывает различные сферы. Для человека, который никогда не сталкивался и не разбирался в подобном вопросе, не так просто представить масштабы этого документа, точнее, размеры и количество сфер и вопросов, которые здесь разрешаются и затрагиваются.

В Доктрине заложены идеи развития и улучшения российского сегмента Интернет и международного стратегического сотрудничества на равных. Некоторые пункты документа посвящены персональной информационной безопасности, личному пространству в сети Интернет, защите личных данных пользователей. И все же одно из основных направлений и важнейший вопрос, который поднимает и пытается решить Доктрина, – кибербезопасность или простым языком, безопасность в Интернете.

Главной стратегической целью документа является защита важных жизненных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях. Важно понимать, что издание доктрины не было прихотью или желанием выделиться на фоне других государств. Это обоснованный шаг для развития и улучшения работы в сети, для безопасного пользования, владения и распоряжения той или иной информацией.

В связи с событиями в мире, ростом преступности, в том числе и в Интернете, возникла необходимость в защите как важных информационных данных производств и государственных служб, так и персональной защите каждого пользователя.

В Доктрине 2000 года раскрывались проблемы в информационной сфере. Отмечалось, что уровень информационной безопасности Российской Федерации не в полной мере соответствует потребностям общества и государства, в интересах защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороноспособности страны и безопасности. Приведем некоторые отрицательные моменты:

- противоречивость и неразвитость правового регулирования общественных отношений в информационной сфере;

- недостаточность нормативного правового регулирования отношений в области реализации возможностей в отношении конституционных ограничений свободы СМИ и т.д.

Особое значение в Доктрине информационной безопасности РФ от 2016 года уделяется ее организационным основам. Принципы деятельности государственных органов по обеспечению информационной безопасности; задачи государственных органов в рамках деятельности по обеспечению информационной безопасности; задачи государственных органов в рамках деятельности по развитию и совершенствованию системы обеспечения информационной безопасности, - это и есть её основы в сокращенном варианте.

И в новой, и в устаревшей версии Доктрин общей проблемой является разложение моральных ценностей молодежи, отток из страны квалифицированных специалистов по безопасности. В доктрине 2000 года в качестве одной из опасностей в информационной сфере значилось "создание монополий на формирование, получение и распространение информации в РФ". Доктрина 2016 года такого положения не содержит. Можно подумать, что причиной исключения этого положения стало решение данной проблемы, но это не так. Развитие сети не стоит на месте, и вместе с этим открывается достаточный выбор способов для создания подобных монополий. Поэтому утверждать, что проблема решена, нельзя. Но можно с уверенностью сказать, что благодаря мерам, которые предпринимались для разрешения этого непорядка, сократилось число преступлений в данном направлении.

Новая Доктрина называет главными угрозами информационной преступности - распространение материалов из-за рубежа, которые нарушают стабильную ситуацию в стране, и популярность давящих на молодежь тенденций. Российские власти считают, что проблема заключается в слабости информационной системы нашей страны, она еще несовершенна для международной конкуренции и нуждается в поддержке со стороны. С этим сложно не согласиться. Россия отстает от ведущих зарубежных стран в области развития информационных технологий и информационных систем, обеспечивающих безопасность.

Из-за непростых отношений с развитыми государствами наша страна пытается развиваться самостоятельно. По ряду причин происходит отток специалистов в другие страны. Данная проблема поднималась в Доктрине 2000 года. Наша страна нуждается в кадрах, которые бы развили данную отрасль. По сравнению с устаревшей версией документа, в доктрине 2016 года акцент делается на опасность «информационно-психологического воздействия» на сознание граждан Российской Федерации со стороны зарубежных спецслужб, не исключая террористические и экстремистские организации.

Стоит заметить, что в доктрине 2000 года не давалось раскрытия понятия - информационная сфера, объяснялось лишь то, что информационная сфера является фактором, который образует систему жизни общества и что она активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации.

Так же в версии 2000 года отсутствовало понятие «экстремистские организации», в качестве угроз были названы «диверсионно-подрывная деятельность иностранных специальных служб» и «деятельность международных террористических организаций».

В доктрине от 05.12.2016 г. добавляется 5 глава. В ее содержание «Основных положений» включены дефиниция Доктрины, основные понятия, используемые в ней, правовая основа, сущность и значение этого документа для государственной политики и общественных отношений в области обеспечения информационной безопасности. Такое изложение, распространенное в структуре большинства законодательных актов, более удобно для восприятия и усвоения его понятий.

Впервые отмечается тенденция к увеличению негативных оценок России в зарубежных СМИ. В предыдущей редакции документа говорилось лишь об "опасности зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур". С одной стороны, можно предположить, что чем сильнее пытается закрепиться наша страна на международной арене, чем больше мы пытаемся развиться хотя бы в одной из сфер, тем больше негативных моментов у нас пытаются найти другие страны. Они критикуют и ограничивают наши новшества, но это лишь доказывает, что Россия стоит на пути развития. С другой стороны, нельзя отрицать того, что наше технологическое развитие значительно отстает от западного и носит во многом имитационный характер.

Доктрина информационной безопасности РФ 2016 года более совершенна по содержанию, чем Доктрина-2000. Но, к сожалению, и ей не удалось избежать

описательного характера, нечеткости, неконкретности определенных терминов, нарушений принципа научности, других специальных принципов общей теорий.

В Доктрине 2000 года было прописано весьма показательное изречение, звучит оно так «Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности». На тот момент у России была цель достичь равенства с другими странами. Как бы то ни было, но в 2016 году эта фраза исчезла.

Состояние информационной безопасности Российской Федерации в экономической области характеризуется отставанием Российской Федерации от ведущих зарубежных государств, в развитии конкурентоспособных информационных технологий, заявили в Совете Безопасности РФ. Тем не менее, пересмотр Доктрины информационной безопасности в 2016 году был необходим. В документе появились новые положения, которые усилили вопросы национальной безопасности государства в информационной сфере, а также безопасность нахождения в сети.

Документы в сфере информационной безопасности федерального уровня можно разделить на три группы: нормативно-правовые (федеральные законы, кодексы и т.д.), организационно-распорядительные (разнообразные стратегии, положения и т.д., утвержденные указами Президента и постановлениями Правительства, а также приказами ФСТЭК России, Гостехкомиссии, Роскомнадзора и т.д.) и нормативно-технические (государственные стандарты).

4. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации

1. Конституция Российской Федерации, принята 12 декабря 1993 года по результатам всенародного голосования, проведённого в соответствии с Указом Президента России от 15 октября 1993 года № 1633 «О проведении всенародного голосования по проекту Конституции Российской Федерации». Она пришла на

смену Основным законам Российской империи 1906 года и конституциям РСФСР 1917 и СССР 1924, 1936 и 1977 годов.

Рассмотрим главные моменты, затрагивающие вопросы информационной безопасности:

Статья 23

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

Статья 24

1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

2. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Статья 29

1. Каждому гарантируется свобода мысли и слова.

2. Не допускаются пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосходства.

3. Никто не может быть принужден к выражению своих мнений и убеждений или отказу от них.

4. Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом.

5. Гарантируется свобода массовой информации. Цензура запрещается.

Статья 42

Каждый имеет право на благоприятную окружающую среду, достоверную информацию о ее состоянии и на возмещение ущерба, причиненного его здоровью или имуществу экологическим правонарушением.

Статья 44

1. Каждому гарантируется свобода литературного, художественного, научного, технического и других видов творчества, преподавания. Интеллектуальная собственность охраняется законом.

2. Каждый имеет право на участие в культурной жизни и пользование учреждениями культуры, на доступ к культурным ценностям.

3. Каждый обязан заботиться о сохранении исторического и культурного наследия, беречь памятники истории и культуры.

2. Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. №646.

I. Общие положения.

1. Настоящая Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

2.Правовую основу настоящей Доктрины составляют Конституция Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, федеральные конституционные законы, федеральные законы, а также нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации.

3.Доктрина является основой для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности.

II. Национальные интересы в информационной сфере.

1.Национальными интересами в информационной сфере являются:

- обеспечение и защита конституционных прав и свобод;
- обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры;
- развитие в Российской Федерации отрасли информационных технологий и электронной промышленности;
- доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации;
- содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам.

2.Реализация национальных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации.

III. Основные информационные угрозы и состояние информационной безопасности.

- Наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях;
- Расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия;
- Различные террористические и экстремистские организации широко используют механизмы информационного воздействия;
- Возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина;
- Состояние информационной безопасности в области науки, технологий и образования характеризуется недостаточной эффективностью научных исследований, направленных на создание перспективных информационных технологий.

IV. Стратегические цели и основные направления обеспечения информационной безопасности.

1.Стратегической целью обеспечения информационной безопасности страны является защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

- защита суверенитета, поддержание политической и социальной стабильности, территориальной целостности Российской Федерации, обеспечение основных прав и свобод человека и гражданина, а также защита критической информационной инфраструктуры;
- пресечение деятельности, наносящей ущерб национальной безопасности Российской Федерации;
- повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры;
- повышение безопасности функционирования объектов информационной инфраструктуры;
- повышение безопасности функционирования образцов вооружения, военной техники.

V. Организационные основы обеспечения информационной безопасности

1.Система обеспечения информационной безопасности строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти.

2.Состав системы обеспечения информационной безопасности определяется Президентом Российской Федерации.

3.Результаты мониторинга реализации настоящей Доктрины отражаются в ежегодном докладе Секретаря Совета Безопасности Российской Федерации

Президенту Российской Федерации о состоянии национальной безопасности и мерах по ее укреплению.

4.Реализация настоящей Доктрины осуществляется на основе отраслевых документов стратегического планирования Российской Федерации.

3. Закон Российской Федерации от 21 июля 1993 года №5485-1 "О государственной тайне" с изменениями и дополнениями, внесенными после его принятия, регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

Статья 2. Основные понятия, используемые в настоящем Законе

В настоящем Законе используются следующие основные понятия:

- государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;
- носители сведений, составляющих государственную тайну, - материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов;
- система защиты государственной тайны - совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях;
- допуск к государственной тайне - процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений;

- доступ к сведениям, составляющим государственную тайну, - санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;
- гриф секретности - реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;
- средства защиты информации - технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.
- Перечень сведений, составляющих государственную тайну, - совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

Статья 28. Порядок сертификации средств защиты информации

Средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Организация сертификации средств защиты информации возлагается на федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области обороны, в соответствии с функциями, возложенными на них законодательством Российской Федерации. Сертификация осуществляется в соответствии с настоящим Законом в порядке, установленном Правительством Российской Федерации (в ред. Федеральных законов от 06.10.1997 N 131-ФЗ, от 30.06.2003 N 86-ФЗ, от 29.06.2004 N 58-ФЗ, от 19.07.2011 N 248-ФЗ). Координация работ по организации сертификации средств

защиты информации возлагается на межведомственную комиссию по защите государственной тайны.

4. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Федеральный закон регулирует отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;

2) применении информационных технологий;

3) обеспечении защиты информации.

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

В 1 статье настоящего Федерального закона используются следующие основные понятия:

1) информация - сведения (сообщения, данные) независимо от формы их представления;

2) информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

3) информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

4) информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

5) обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

6) доступ к информации - возможность получения информации и ее использования;

7) конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

8) предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

9) распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

10) электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

11) документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

12) оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Статья 16. Защита информации

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

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

2) соблюдение конфиденциальности информации ограниченного доступа,

3) реализацию права на доступ к информации.

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

3. Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3 части 1 настоящей статьи.

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

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации.

5. Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных

систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

6. Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

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

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

2. Лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации. Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством Российской Федерации требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

3. В случае, если распространение определенной информации ограничивается или запрещается федеральными законами, гражданско-правовую ответственность за распространение такой информации не несет лицо, оказывающее услуги:

1) либо по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений;

2) либо по хранению информации и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения информации.