МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ГОСУДАРСТВА И ПРАВА
Кафедра административного и финансового права

РЕКОМЕНДОВАНО К ЗАЩИТЕ
В ГЭК И ПРОВЕРЕНО НА ОБЪЕМ
ЗАИМСТВОВАНИЯ
Заведующий кафедрой
канд. юрид. наук, доцент
_____С.В. Горовенко
15 06 2017г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

АДМИНИСТРАТИВНО-ПРАВОВЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

40.04.01 Юриспруденция
Магистерская программа
«Правовая организация деятельности органов публичной власти»

Выполнил работу
студент 2 курса
очной формы обучения — Козлов Даниил Евгеньевич

Научный руководитель
канд. юрид. наук, доцент — Костылев Анатолий Кронидович

Рецензент
Заместитель директора департамента
имущественных отношений
Тюменской области — Третьяков Владимир Сергеевич

Тюмень, 2017

СОДЕРЖАНИЕ

СПИСОК СОКРАЩЕНИЙ

АБС	–	Автоматизированная банковская система
АНБ США	–	Агентство национальной безопасности Соединенных Штатов Америки
ГФС РФ	–	Государственная фельдъегерская служба Российской Федерации
ИБ	–	Информационная безопасность
ИСПДн	–	Информационная система персональных данных
МВД РФ	–	Министерство внутренних дел Российской Федерации
МО РФ	–	Министерство обороны Российской Федерации
НСД	–	Несанкционированный доступ
ПДн	–	Персональные данные
СВР РФ	–	Служба внешней разведки Российской Федерации
СМИ	–	Средства массовой информации
ФСБ РФ	–	Федеральная служба безопасности Российской Федерации
ФСО РФ	–	Федеральная служба охраны Российской Федерации
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю России

ВВЕДЕНИЕ

Окружающий нас мир стремительно становится цифровым. Через информационно-телекоммуникационные сети органы государственной власти осуществляют свою деятельность, хранят и обрабатывают секретную информацию и информацию с ограниченным доступом от целостности, которой может зависеть национальная безопасность целого государства. Например, секретные научные разработки в области обороны, медицины, науки или стратегически важная информация о расположении вооруженных сил, в том числе расположение или коды доступа к запуску ядерного оружия.

В настоящее время информация является одним из наиболее важных стратегических ресурсов. Каждое государство старается обеспечить эффективную защиту для сохранности информации с ограниченным доступом, ведь обеспечение информационной безопасности входит в систему национальной безопасности любого государства.

Так как процесс информатизации стремительно развивается, то большинство конфиденциальной информации хранится в электронном виде. Однако это также несет и определенные угрозы со стороны подготовленных лиц или зарубежных спецслужб, которые при наличие определённых знаний, а также необходимых технических средств, включая специальное программное обеспечение могут получить несанкционированный доступ к конфиденциальной информации и использовать ее в каких-то своих целях.

Информационно-телекоммуникационная сеть «Интернет» с ее огромным количеством положительных функций и возможностей, таких как доступ к электронным библиотекам практически с любой литературой, возможность беспрепятственно общаться, обмениваться информацией с людьми из любой точки планеты и множество других возможностей, так и использование сети с целью координации деятельности террористических организаций, распространения своих экстремистских взглядов и вербовка в свои ряды, совершения кражи персональных

данных, осуществления мошеннических операций с использованием банковских кар или анонимная торговля наркотическими средствами и т.д.

В погоне за секретной информацией спецслужбы зарубежных стран разрабатывают и внедряют специальные программы слежения и системы перехвата информации, в том числе и в отношении граждан своей страны, что является нарушением прав человека.

Процесс обеспечения информационной безопасности постепенно смещается в сторону электронных технологий создания, хранения и передачи данных.

Вопросами обеспечения информационной безопасности в разные годы занимались такие исследователи как В.Н. Лопатин, И.Л. Бачило, В.И. Ярочкин, В.А. Галатенко, С.Ю. Соболь, П.А. Шариков, Т.А. Полякова, А.А. Стрельцов, Я.С. Артамонова, О.С. Макаров и другие.

Актуальность выбранной темы заключается в том, что информация повсюду вокруг нас. За последний год была принята новая Доктрина информационной безопасности Российской Федерации, в действующее законодательство были введены поправки. Стали известны факты слежения Соединенными Штатами как за собственными гражданами, так и за лидерами европейских стран. В стремительно развивающейся информационной сфере необходимо уделять пристальное внимание обеспечению информационной безопасности. С помощью современных технологий можно манипулировать общественным сознанием, собирать огромное количество народа в одном месте с различными целями. Подобные процессы необходимо контролировать и своевременно реагировать на действия, которые несут угрозу как конституционному строю, так и национальной безопасности.

Объектом исследования является информационная безопасность Российской Федерации.

Предметом исследования выступают административно-правовые нормы обеспечения информационной безопасности Российской Федерации.

Целью исследования является анализ нормативных правовых актов Российской Федерации и разработка рекомендаций для повышения эффективности мер обеспечения информационной безопасности.

Для достижения цели необходимо решить следующие **задачи**:

–Проанализировать действующее законодательство Российской Федерации в области информационной безопасности;

–Рассмотреть субъекты обеспечивающие информационную безопасность Российской Федерации;

–Провести анализ зарубежного опыта в обеспечении информационной безопасности;

–Раскрыть характеристику угроз информационной безопасности Российской Федерации;

–Исследовать меры по обеспечению информационной безопасности Российской Федерации, дать рекомендации к улучшению мер.

При написании диссертации были использованы такие методы исследования как системный подход и сравнительный анализ, а также обобщение статистических данных.

Структура работы состоит из введения, двух глав и пяти параграфов, заключения и списка литературы.

В первой главе «Теоретико-правовые основы информационной безопасности Российской Федерации», в первом параграфе раскрыто понятие информационной безопасности Российской Федерации и рассмотрено правовое регулирование обеспечения информационной безопасности Российской Федерации. Второй параграф первой главы содержит структуру субъектов обеспечивающих информационную безопасность личности, общества и государства. В третьем параграфе приведен анализ зарубежного опыта обеспечения информационной безопасности на примере Соединенных Штатов Америке и сделаны соответствующие выводы.

Во второй главе «Проблемы обеспечения информационной безопасности Российской Федерации», в первом параграфе охарактеризованы угрозы информационной безопасности Российской Федерации, приведены статистические данные. Второй параграф содержит исследование мер по обеспечению

информационной безопасности Российской Федерации, а также даны необходимые рекомендации.

ГЛАВА 1. ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

1.1Понятие и правовое регулирование обеспечения информационной безопасности Российской Федерации.

Понятие «информационная безопасность» стало актуальным и приобрело значимость с того момента, когда началось активное развитие информационных и телекоммуникационных технологий. Уже тогда становится понятным то, что без использования информационных технологий невозможно обеспечить развитие, а также экономический рост любого государства и выполнять быстро и качественно осуществление государством своих функций.

По мнению И.Л. Бачило «под информационной безопасностью понимается состояние всех компонентов информационных ресурсов, технологий и коммуникаций, – позволяющее осуществлять их формирование и использование в интересах общества, государства и человека при минимизации отрицательных последствий для создателей, держателей и пользователей этих ресурсов, возникающих под влиянием внутренних и внешних угроз»[1].

В своем научном исследовании А.А. Стрельцов понятие «информационная безопасность» предлагает раскрыть как невозможность нанесения вреда, в следствии возникновения угроз[2].

В Диссертационном исследовании В.Н. Лопатина под информационной безопасностью предлагается понимать состояние защищенности национальных интересов страны (жизненно важных интересов личности, общества и государства на сбалансированной основе) в информационной сфере от внутренних и внешних угроз[3].

---

[1] Бачило И. Л. Информационное право: учебник. М.: Юрайт, 2016. С. 375.

[2] Стрельцов А.А. Теоретические и методологические основы правового обеспечения информационной безопасности России: автореф. дис. ... докт. юрид. наук: 05.13.19 / А.А. Стрельцов. М., 2004. С. 19

[3] Лопатин В. Н. Информационная безопасность России: Человек, общество, государство. М., 2000. С. 13.

И. Ю. Гольтяпина в своем исследование не согласна с тем, что информационную безопасность относят лишь в отношении к жизненно важным интересам, ведь какие тогда интересы не являются жизненно важными и почему в отношении их не нужно обеспечивать безопасность. Автор формулирует определение информационной безопасности как состояние защищенности законных интересов субъектов в информационной сфере от внутренних и внешних угроз[4].

Коллектив авторов А.П. Купило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой информационную безопасность определяют, как «состояние защищенности информации, которое достигается обеспечением совокупности для нее свойств доступности, целостности, конфиденциальности, аутентичности, подотчетности и надежности»[5].

Я.С. Артамонова под информационной безопасностью предлагает понимать такое состояние информационного пространства страны, при котором его основным характеристикам: целостности, доступности и конфиденциальности, - ничего не угрожает и обеспечена достаточно надежная защита от угрозы[6].

Согласно обновленной Доктрине информационной безопасности Российской Федерации, принятой указом Президента РФ от 05.12.2016 г. N 646, под информационной безопасностью определяется – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства. В свою очередь под обеспечением информационной безопасности понимается - осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-

---

[4] Гольтяпина И.Ю. Административно-правовые средства обеспечения информационной безопасности в России: автореф. дис. ... канд. юрид. наук: 12.00.14 / И.Ю. Гольтяпина. Омск, 2008. С. 16.

[5] Курило А.П., Милославская Н.Г., Сенаторов М.Ю. Основы управления информационной безопасностью. Учебное пособие для вузов. М., 2016. С. 30.

[6] Артамонова Я.С. Информационная безопасность российского общества: теоретические основания и практика политического обеспечения: автореф. дис. ... докт. полит. наук: 23.00.02 / Я.С. Артамонова. М., 2014. С. 26.

аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления[7].

До 2016 года действовала предыдущая Доктрина информационной безопасности Российской Федерации утверждена Президентом РФ от 09.09.2000 г. N Пр-1895[8] (Документ утратил силу с 5 декабря 2016 года в связи с изданием Указа Президента РФ от 05.12.2016 N 646). В ней приведено следующее определение информационной безопасности - это состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства. Сравнив понятия можно сделать вывод, что в действующей Доктрине информационной безопасности Российской Федерации дано более развернутое понятие «информационная безопасность». Однако, можно предположить, что при формулировке основного понятия было скопировано определение «национальной безопасности», которое закреплено в Стратегии национальной безопасности Российской Федерации, с заменой слова «национальная» на «информационная»[9].

Правовую основу обеспечения информационной безопасности Российской Федерации, помимо упомянутой выше Доктрины информационной безопасности Российской Федерации, составляют Конституция Российской Федерации[10], в которой в статьях 23, 24, 29, 42, 44 закреплены основные права и свободы граждан в информационно сфере, Федеральные законы, Указы и распоряжения Президента Российской Федерации, Постановления Правительства Российской Федерации, Документы уполномоченных федеральных органов (ФСБ, ФСТЭК, Роскомнадзор),

---

[7] Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 05.12.2016 г. N 646: по сост. на 30 марта 2017 г. // Собрание законодательства РФ. –2016. – N 50. – Ст. 7074.

[8] Доктрина информационной безопасности Российской Федерации: утв. Президентом РФ от 09.09.2000 г. N Пр-1895 // Российская газета. – N 187. – 2000. (Документ утратил силу с 5 декабря 2016 года в связи с изданием Указа Президента РФ от 05.12.2016 N 646).

[9] Молчанов Н.А., Матевосова Е.К. Доктрина информационной безопасности Российской Федерации (новелла законодательства) // Актуальные проблемы российского права. 2017. N 2. С. 61.

[10] Конституция Российской Федерации принята всенародным голосованием 12 декабря 1993 г.: по сост. на 21 июля 2014 г. // Собрание законодательства РФ. – 2014. – № 31. – Ст. 4398.

Национальные стандарты в области информационной безопасности, Нормативно-методические и руководящие документы.

Федеральный закон «О безопасности» № 390-ФЗ определяет основные принципы и содержание деятельности по обеспечению безопасности государства, общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством Российской Федерации, полномочия и функции федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления в области безопасности[11]. Хотя в законе прямо не указано, что он определяет принципы и содержание деятельности по обеспечению информационной безопасности, это подразумевается в формулировке «иных видов безопасности».

Указом Президента РФ от 31.12.2015г. № 683 утверждена Стратегия национальной безопасности Российской Федерации[12]. В Связи с этим признана утратившей силу предыдущая Стратегия национальной безопасности Российской Федерации до 2020 года, утвержденная в 12.05.2009 г., и с внесенными изменениями от 01.07.2014 г.

Стратегия является базовым документом стратегического планирования, определяющим национальные интересы и стратегические национальные приоритеты Российской Федерации, цели, задачи и меры в области внутренней и внешней политики, направленные на укрепление национальной безопасности Российской Федерации и обеспечение устойчивого развития страны на долгосрочную перспективу.

Настоящая Стратегия является основой для формирования и реализации государственной политики в сфере обеспечения национальной безопасности Российской Федерации[13].

---

[11] О безопасности: федеральный закон от 28.12.2010 г. N 390-ФЗ: по сост. на 25 апреля 2017 г. // Собрание законодательства РФ. – 2011. – N 1. – Ст. 2.

[12] О Стратегии национальной безопасности Российской Федерации: указ Президента РФ от 31.12.2015 г. N 683: по сост. на 12 апреля 2017 г. // Собрание законодательства РФ. – 2016. – N 1 (часть II). – Ст. 212.

[13] Собрание законодательства РФ. – 2016. – N 1 (часть II). – Ст. 212.

В современный период информационная безопасность общества стала неотъемлемой частью национальной безопасности. В Стратегии национальной безопасности России, утвержденной Указом Президента от 31 декабря 2015г. N683, в п. 22 отмечается появление новых форм противоправной деятельности, в частности с использованием информационных, коммуникационных и высоких технологий. Одной из угроз военной безопасности РФ является развитие информационных средств ведения войны[14].

Реализация настоящей Стратегии призвана способствовать развитию национальной экономики, улучшению качества жизни граждан, укреплению политической стабильности в обществе, обеспечению обороны страны, государственной и общественной безопасности, повышению конкурентоспособности и международного престижа Российской Федерации[15].

Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 года N646, является документом стратегического планирования в сфере обеспечения национальной безопасности Российской Федерации, в котором развиваются положения Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 31 декабря 2015г. N683, а также других документов стратегического планирования в указанной сфере.

Действующая Доктрина информационной безопасности Российской Федерации подробно раскрывает понятие «национальные интересы Российской Федерации в информационной сфере» – это объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы. Также дается перечень, что конкретно является национальными интересами в информационной сфере. В Доктрине информационной безопасности Российской Федерации 2000 года подробно не раскрывалось понятие «информационная сфера».

---

[14] Степанов-Егиянц В.Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации: монография. М.: Статут, 2016. С. 8

[15] Собрание законодательства РФ. – 2016. – N 1 (часть II). – Ст. 212.

В главе третьей перечисляются основные информационные угрозы и состояние информационной безопасности Российской Федерации, говорится о том, что одним из основных негативных факторов, влияющих на состояние информационной безопасности, является наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях. Отмечается тенденция к увеличению в зарубежных средствах массовой информации объема материалов, содержащих предвзятую оценку государственной политики Российской Федерации. Российские средства массовой информации зачастую подвергаются за рубежом откровенной дискриминации, российским журналистам создаются препятствия для осуществления их профессиональной деятельности[16]. Хоть в содержании Доктрины и не указываются страны, которые несут основную угрозу нашему государству, и которые представляют угрозу, в том числе информационной безопасности Российской Федерации, эти страны давно известны. Эти страны уже на протяжении долгих лет остаются серьезным противником национальной безопасности нашей страны в целом.

Стратегической целью обеспечения информационной безопасности в области обороны страны является защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности.

Также в Доктрине информационной безопасности Российской Федерации перечисляются основные цели и направления обеспечения информационной безопасности такие как:

–в области обороны страны;

[16] Собрание законодательства РФ. –2016. – N 50. – Ст. 7074.

–в области государственной и общественной безопасности;

–в экономической сфере;

–в области науки, технологий и образования;

–в области стратегической стабильности и равноправного стратегического партнерства.

Одним из ключевых направлений обеспечения информационной безопасности любого государства, является защита и охрана государственной тайны. Положения по защите и охране государственной тайны нашей страны закреплены в Законе Российской Федерации «О государственной тайне», принятым 21.07.1993г. № 5485-1. В соответствии с Законом под государственной тайной понимается - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации[17].

В Статье 5 Закона О государственной тайне содержится перечень сведений, составляющих государственную тайну– это сведения в военной области (о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, предусмотренных Федеральным законом «Об обороне», об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов; о планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники; о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов, их составных частей, делящихся

[17] Собрание законодательства РФ. – 1997 г. – N 41. – Стр. 8220-823.

ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения и т.д.); сведения в области экономики, науки и техники (о содержании планов подготовки Российской Федерации и ее отдельных регионов к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов; об использовании инфраструктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства; о силах и средствах гражданской обороны, о дислокации, предназначении и степени защищенности объектов административного управления, о степени обеспечения безопасности населения, о функционировании транспорта и связи в Российской Федерации в целях обеспечения безопасности государства и т.д.); сведения в области внешней политики и экономики (о внешнеполитической, внешнеэкономической деятельности Российской Федерации, преждевременное распространение которых может нанести ущерб безопасности государства; о финансовой политике в отношении иностранных государств (за исключением обобщенных показателей по внешней задолженности), а также о финансовой или денежно-кредитной деятельности, преждевременное распространение которых может нанести ущерб безопасности государства); сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму и в области обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты (о силах, средствах, об источниках, о методах, планах и результатах разведывательной, контрразведывательной, оперативно-розыскной деятельности и деятельности по противодействию терроризму, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения; о силах, средствах, об источниках, о методах, планах и результатах деятельности по

обеспечению безопасности лиц, в отношении которых принято решение о применении мер государственной защиты, данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения, а также отдельные сведения об указанных лицах; о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность и т.д.).

Статья 7 содержит сведения, не подлежащие отнесению к государственной тайне и засекречиванию. Сведения следующего характера:

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

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

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

–о фактах нарушения прав и свобод человека и гражданина;

–о размерах золотого запаса и государственных валютных резервах Российской Федерации;

–о состоянии здоровья высших должностных лиц Российской Федерации;

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

Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений. Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для

носителей указанных сведений: «особой важности», «совершенно секретно» и «секретно»[18].

В соответствии с пунктом третьим правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности, к сведениям особой важности следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из перечисленных областей.

К совершенно секретным сведениям следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам министерства (ведомства) или отрасли экономики Российской Федерации в одной или нескольких из перечисленных областей.

К секретным сведениям следует относить все иные сведения из числа сведений, составляющих государственную тайну. Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесенный интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-розыскной области деятельности[19].

В ст.20 перечислены органы защиты государственной тайны, ранжированные в порядке полномочий, закрепляемых за ними.

Возглавляет данный перечень Межведомственная комиссия, руководство деятельностью которой осуществляет Президент РФ. Далее следуют уполномоченные федеральные органы исполнительной власти в соответствующих областях защиты государственной тайны (в области обеспечения безопасности-

[18] Собрание законодательства РФ. – 1997 г. – N 41. – Стр. 8220-823.

[19] Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности: постановление Правительства РФ от 04.09.1995 г. N 870: по сост. на 13 апреля 2017 г. // Собрание законодательства РФ. – 1995. – N 37. – Ст. 3619.

Федеральная служба безопасности, в области обороны- Министерство обороны РФ, в области внешней разведки- Служба внешней разведки РФ, в области противодействия техническим разведкам и технической защиты информации- Федеральная служба по техническому и экспортному контролю). Указанные четыре области интересов государства непосредственно связаны с обеспечением его безопасности и обороноспособности. Замыкают перечень органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите государственной тайны[20].

Основной деятельностью этих органов является защита государственной тайны.

Система нормативных актов, определяющая сведения, отнесенные к государственной тайне выглядит так:

Закон «О государственной тайне» содержит категории сведений, составляющих государственную тайну; Указом Президента РФ № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне»[21], утвержден перечень этих сведений, который определяет для распоряжения каждой категорией, указанной в Законе, государственный орган (всего 118 пунктов); Руководство государственных органов, закрепленных в Указе Президента РФ № 1203, в соответствии перечня сведений Закона «О государственной тайне» составляют и утверждают секретными приказами свои развернутые перечни сведений, подлежащих засекречиванию, включая в них еще более детализированные категории сведений, которые находятся в компетенции этих органов[22].

Одним из важнейших элементов рыночной экономики является коммерческая тайна. В связи с постоянно растущем уровнем конкуренции данному ресурсу всегда уделялось особое внимание в целях ограничения доступа третьих лиц, будь то

---

[20] Спектор Е.И. Комментарий к Закону Российской Федерации «О государственной тайне» (постатейный). М.: Юстицинформ, 2006. С. 83.

[21] Об утверждении Перечня сведений, отнесенных к государственной тайне: указ Президента РФ от 30.11.1995 г. N 1203: по сост. на 14 апреля 2017 г. // Собрание законодательства РФ. – 1995. – N 49. – Ст. 4775.

[22] Павлов И.Ю. Современные проблемы правового регулирования государственной и служебной тайны в России // Ленинградский юридический журнал. 2013. № 1 (31). С. 31.

особая технология производства или традиционный секрет ремесла региона или даже целой страны.

В российском законодательстве основные положения закреплены в Федеральном законе N 98-ФЗ «О коммерческой тайне» от 29.07.2004 г., который регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам.

Названный федеральный закон определяет коммерческую тайну как режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду. Также дается определение информации, составляющей коммерческую тайну - сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны[23].

К признакам, содержащим понятие «коммерческая тайна» можно отнести- конфиденциальность сведений, то есть скрытость от третьих лиц; ценность этих сведений, в связи с неизвестностью третьим лицам.

Разглашением коммерческой тайны в соответствии с статьей 3 федерального закона «О коммерческой тайне» является действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических

---

[23] О коммерческой тайне: федеральный закон от 29.07.2004 г. N 98-ФЗ: по сост. на 16 апреля 2017 г. // Собрание законодательства РФ. – 2004. – N 32. – Ст. 3283.

средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

В соответствии со статьей 12 Федерального закона N 335-ФЗ «Об инвестиционном товариществе»[24] к коммерческой тайне также относятся и не разглашаются условия договора инвестиционного товарищества.

К сведениям, относящимся к коммерческой тайне, осуществляется особый режим допуска, т.е. работника обязаны ознакомить под расписку с информацией, составляющей коммерческую тайну, обладателем которой является организация. Также под расписку ознакомить с установленным режимом и ответственностью за нарушение режима и создать благоприятные условия соблюдения данного режима.

Очень обширный круг сведений предпринимательской деятельности может составлять коммерческую тайну. Предприниматель, имеющий в своем распоряжении конфиденциальную информацию, на сам вправе устанавливать объем и состав сведений, порядок использования, доступа и защиты коммерческой тайны.

Разглашение коммерческой тайны для любой организации либо предприятия понесет значительные убытки деятельности с экономической точки зрения.

Одним из видов тайн, которые охраняются в Российской Федерации является банковская тайна. Это закреплено в статье 26 Федерального закона от 02.12.1990 №395-1 «О банках и банковской деятельности»[25] и в статье 857 ГК РФ.

Субъектами банковской тайны являются клиенты (физические и юридические лица) и сами кредитные организации.

Как следует из статьи 26 Федерального закона от 02.12.1990 №395-1 «О банках и банковской деятельности» под банковской тайной следует понимать сведения физических и юридических лиц об операциях по счетам; о счетах и вкладах в банке (кредитной организации); о балансе и переводах электронных денежных средств; персональные данные клиента.

---

[24] Об инвестиционном товариществе: федеральный закон от 28.11.2011 г. N 335-ФЗ: по сост. на 16 апреля 2017 г. // Собрание законодательства РФ. – 2011. – N 49 (ч. 1). – Ст. 7013.

[25] О банках и банковской деятельности: федеральный закон от 02.12.1990 г. N 395-1: по сост. на 16 апреля 2017 г. // Собрание законодательства РФ. –1996. – N 6. – ст. 492.

Банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте[26] (ст. 857 ГК РФ).

За разглашение банковской тайны Банк России, руководители (должностные лица) федеральных государственных органов, перечень которых определяется Президентом Российской Федерации, высшие должностные лица субъектов Российской Федерации (руководители высших исполнительных органов государственной власти субъектов Российской Федерации), организация, осуществляющая функции по обязательному страхованию вкладов, кредитные, аудиторские и иные организации, уполномоченный орган, осуществляющий функции по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, орган валютного контроля, уполномоченный Правительством Российской Федерации, и агенты валютного контроля, а также должностные лица и работники указанных органов и организаций несут ответственность, включая возмещение нанесенного ущерба, в порядке, установленном федеральным законом.

Операторы платежных систем не вправе раскрывать третьим лицам информацию об операциях и о счетах участников платежных систем и их клиентов, за исключением случаев, предусмотренных федеральными законами.

Статья 26 ФЗ №395-1 «О банках и банковской деятельности» также содержит, что справки по счетам и вкладам физических лиц выдаются кредитной организацией им самим, судам, органам принудительного исполнения судебных актов, актов других органов и должностных лиц, организации, осуществляющей функции по обязательному страхованию вкладов, при наступлении страховых случаев, предусмотренных федеральным законом о страховании вкладов физических лиц в банках Российской Федерации, а при наличии согласия руководителя следственного органа - органам предварительного следствия по делам, находящимся в их производстве. Это означает, что банковская тайна неразрывно связана с такими понятием как «персональные данные».

---

[26] Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 г. N 14-ФЗ: по сост. на 18 апреля 2017 г. // Собрание законодательства РФ. –1996. – N 5. – Ст. 410.

Не так давно был принят Федеральный закон N 152-ФЗ от 27.07.2006г. «О персональных данных», целью которого является обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну[27].

Информация о частной жизни человека начала актуализироваться в период массовой информатизации жизни, когда эти сведения необходимо было вводить в автоматизированные информационные системы в целях повышения эффективности функционирования государственных органов и коммерческих организаций.

Под персональными данными законодатель считает любую информацию, относящуюся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

Как следует из понятия ключевым признаком является то, что с помощью таких сведений можно не только выделить конкретного человека из множества других, но и точно его идентифицировать. Также важным признаком персональных данных является то, что это сведения о фактах, событиях и обстоятельствах жизни человека, обладающие ценностными характеристиками. Это сведения, которые определяют не только его внешние качества, но и внутренние свойства, в том числе и биометрические данные (ДНК, отпечатки пальцев, рост, походка, голос и т.д.)[28].

Конфиденциальность персональных данных осуществляется посредством того, что операторы и иные лица, получившие доступ к ПДн, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

В соответствии с законодательством персональные данные не являются тайной, это информация ограниченного доступа, поскольку при согласии субъекта могут передаваться третьим лицам. Тем не менее они требуют высокой степени защиты как, например, государственная или коммерческая тайна.

---

[27] О персональных данных: федеральный закон от 27.07.2006 г. N 152-ФЗ: по сост. на 23 апреля 2017 г. // Собрание законодательства РФ. – 2006. – N 31 (1 ч.). – Ст. 3451.

[28] Кузнецов П. У. Основы информационного права учебник: для студентов высших учебных заведений. М..: Проспект, 2014. С. 261-262

Одним из базовых законов, который регулирует отношения, возникающие при осуществлении поиска, получения, передачи и распространении информации, а также содержит общие условия защиты информации является Федеральный закон N 149-ФЗ от 27.07.2006г. «Об информации, информационных технологиях и о защите информации»[29].

Федеральный закон N 149-ФЗ в ст. 7 к общедоступной информации относит общеизвестные сведения и иную информация, доступ к которой не ограничен. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

В соответствии со ст.9 ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами (персональные данные, государственная, коммерческая, банковская тайны и т.д.).

В статье 10.1 названного закона закреплено, что лицо, осуществляющее деятельность по обеспечению функционирования информационных систем или программ для электронных вычислительных машин, которые используются для приема, передачи, доставки и обработки электронных сообщений пользователей сети «Интернет» (Организатор распространения информации в сети «Интернет») обязано хранить на территории Российской Федерации: информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей сети «Интернет» и информацию об этих пользователях в течение одного года с момента окончания осуществления таких действий; а также текстовые сообщения пользователей сети «Интернет», голосовую информацию, изображения,

[29] Об информации, информационных технологиях и о защите информации: федеральный закон от 27.07.2006 г. N 149-ФЗ: по сост. на 28 апреля 2017 г. // Собрание законодательства РФ. – 2006 г. – N 31 (1 ч.). – Ст. 3448.

звуки, видео-, иные электронные сообщения пользователей сети «Интернет» до 6 месяцев с момента окончания их приема, передачи, доставки и (или) обработки.

С 1 сентября 2012 года вступил в силу Федеральный закон N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»[30]. Данный закон был принят с целью ограничить подрастающее поколение граждан от информации, в том числе информационной продукции, которая способна нанести вред психическому, а также физическому здоровью и развитию ребенка. К такой информации законодатель относит сведения следующего характера это побуждающие детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству; способные вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством; обосновывающие или оправдывающие допустимость насилия и (или) жестокости либо побуждающие осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом; отрицающие семейные ценности, пропагандирующие нетрадиционные сексуальные отношения и формирующие неуважение к родителям и (или) другим членам семьи; оправдывающие противоправное поведение; содержащие нецензурную брань; содержащие информацию порнографического характера; о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего.

---

[30] О защите детей от информации, причиняющей вред их здоровью и развитию: федеральный закон от 29.12.2010 N 436-ФЗ: по сост. на 22 апреля 2017 г. // Собрание законодательства РФ. – 2011. – N 1. – Ст. 48.

В гл.2 Федеральный закон классифицирует информационные продукты в зависимости от возраста детей: до 6 лет, от 6 до 12 лет, от 12 до 16 лет. Классификацию самих информационных продуктов должен проводить производитель, оценивая жанр, тематику продукта, его оформление и содержание, особенности восприятия информации детей разного возраста. Также закрепляются требования к обороту такой продукции через средства массовой информации и информационно-телекоммуникационную сеть «Интернет».

Рассмотренные выше нормативно-правовые акты не являются исчерпывающими в системе обеспечения информационной безопасности Российской Федерации. Данные документы, по нашему мнению, занимают ключевое положение в регулировании основных сфер деятельности общества и государства. Основной проблемой является то, что на данный момент до сих пор существуют разногласия в понимании термина «информационная безопасность» и разные авторы предлагают своё понимание данного термина.

В новой Доктрине информационной безопасности Российской Федерации законодатель попытался дать точное определение информационной безопасности «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства», однако данное определение совпадает с определением «национальная безопасность Российской Федерации», закрепленным в Стратегии национальной безопасности Российской Федерации от 31 декабря 2015 года «состояние защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан Российской Федерации, достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации» добавилось слово «информационных».

1.2 Субъекты, обеспечивающие информационную безопасность личности, общества и государства.

Чтобы обеспечивать информационную безопасность целого государства должна быть четкая система органов государственной власти, в которой каждый орган государственной власти будет осуществлять конкретные функции, в пределах своей компетенции, по обеспечению информационной безопасности.

В настоящее время система органов государственной власти выглядит следующим образом.

Президент Российской Федерации, в пределах своих конституционных полномочий, осуществляет руководство органами государственной власти по обеспечению информационной безопасности Российской Федерации. Формирует, проводит реорганизацию, а также упраздняет, в соответствии с законодательством Российской Федерации, подчиненные ему органы власти по обеспечению информационной безопасности. В своем ежегодном послании Федеральному Собранию определяет ключевые направления государственной политики в сфере обеспечения информационной безопасности государства.

Совет Федерации и Государственная Дума в соответствии с Конституцией по представлению Президента и Правительства Российской Федерации вырабатывают законодательную базу в сфере обеспечения информационной безопасности Российской Федерации.

Структурным подразделением Государственной Думы Федерального Собрания Российской Федерации по вопросам предварительного рассмотрения и подготовке к рассмотрению Государственной Думой законопроектов и проектов постановлений палаты о статусе и правовом регулировании деятельности: СВР РФ, МВД РФ, ФСО РФ, ФСБ РФ и др., является Комитет Государственной Думы по безопасности и противодействию коррупции[31]. Также Комитет ГД предварительно

[31] Положение о Комитете Государственной Думы Федерального Собрания Российской Федерации по безопасности и противодействию коррупции утверждено решением Комитета Государственной Думы по безопасности и противодействию коррупции: протокол № 15/8, утверждено решением Комитета Государственной Думы по

рассматривает и подготавливает к рассмотрению Государственной Думой законопроекты и проекты постановлений палаты по вопросам информационной безопасности личности, общества и государства (защиты информации, составляющей государственную, служебную и коммерческую тайну, защита персональных данных, информационно-психологическая безопасность человека).

Правительство Российской Федерации координирует работу федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации с учетом положений ежегодного послания Президента Российской Федерации Федеральному Собранию и в пределах своих полномочий. При формировании федерального бюджета, выделяет средства для реализации направлений деятельности в обеспечении информационной безопасности.

В соответствии с положением о Совете безопасности Российской Федерации, утвержденным указом Президента Российской Федерации 6 мая 2011 г. N 590[32] Совет безопасности осуществляет подготовку решений Президента Российской Федерации по вопросам обеспечения информационной безопасности и национальной безопасности в целом; обеспечивает необходимые условия для осуществления Президентом Российской Федерации полномочий в области обеспечения информационной безопасности; проводит оценку эффективности, разработку критериев и показателей деятельности федеральных органов исполнительной власти в области обеспечения информационной безопасности; реформирует существующие или принимает решение об образовании новых государственных органов и организаций, осуществляющих функции в области обеспечения информационной безопасности; проводит стратегическую оценку состояния информационной безопасности Российской Федерации и развития информационного общества в Российской Федерации, а также деятельность федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации в области обеспечения информационной

безопасности и противодействию коррупции от 17 января 2017 г. [Электронный ресурс]. URL: http://www.komitet2-16.km.duma.gov.ru/Polozhenie-i-voprosy-vedeniya/ (дата обращения 27.03. 2017 г.).

[32] Положение о Совете Безопасности Российской Федерации: указ Президента РФ от 06.05.2011 г. N 590: по сост. на 30 марта 2017 г. // Собрание законодательства РФ. – 2011. – N 19. – Ст. 2721.

безопасности; координирует деятельность федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации по реализации принятых Президентом Российской Федерации решений в области обеспечения информационной безопасности; разрабатывает и уточняет критерии и показатели обеспечения информационной безопасности; рассматривает проекты законодательных и иных нормативных правовых актов Российской Федерации по вопросам, входящим в компетенцию Совета Безопасности; подготавливает проекты нормативных правовых актов Президента Российской Федерации по вопросам обеспечения информационной безопасности, организации обороны и осуществления контроля деятельности федеральных органов исполнительной власти в области обеспечения безопасности; организовывает разработку федеральных (государственных) целевых программ в области обеспечения информационной безопасности и осуществляет контроль их реализации.

В целях реализации, возложенных на Совет Безопасности Российской Федерации задач в области обеспечения информационной безопасности образована Межведомственная комиссия Совета Безопасности Российской Федерации по информационной безопасности[33], которая подготавливает предложения и рекомендации Совету Безопасности по выработке и реализации основных направлений государственной политики в области обеспечения информационной безопасности Российской Федерации а также предложения и рекомендации по координации деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации по реализации федеральных целевых программ и исполнению решений Совета Безопасности в области обеспечения информационной безопасности Российской Федерации; анализирует информацию о состоянии информационной безопасности Российской Федерации и подготавливает предложения и рекомендации Совету Безопасности по совершенствованию деятельности федеральных органов исполнительной власти,

[33] Положение о Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности: указ Президента РФ от 06.05.2011 г. N 590: по сост. на 03 апреля 2017 г. // Собрание законодательства РФ. – 2011. – N 19. – Ст. 2721.

органов исполнительной власти субъектов Российской Федерации в области обеспечения информационной безопасности Российской Федерации, а также анализирует состояние информационной безопасности информационно-телекоммуникационных систем и сетей критически важных объектов инфраструктуры и вырабатывает предложения и рекомендации федеральным органам исполнительной власти по повышению уровня их защищенности; осуществляет прогноз, оценку и выявление угроз информационной безопасности Российской Федерации, их источников, подготавливает предложения и рекомендации Совету Безопасности по предотвращению выявленных и недопущению прогнозируемых угроз в области обеспечения информационной безопасности Российской Федерации; рассматривает проектов федеральных целевых программ, направленных на обеспечение информационной безопасности Российской Федерации, подготавливает соответствующие предложения и рекомендации Совету Безопасности; участвует в подготовке материалов по вопросу обеспечения информационной безопасности Российской Федерации для ежегодного послания Президента Российской Федерации Федеральному Собранию Российской Федерации, подготавливает предложения и рекомендации Совету Безопасности по вопросам организации стратегического планирования в Российской Федерации; предложения и рекомендации Совету Безопасности по разработке проектов нормативных правовых актов, направленных на обеспечение информационной безопасности Российской Федерации.

Министерство обороны Российской Федерации (МО РФ), являясь исполнительным органов Российской Федерации, осуществляет функции по выработке и реализации государственной политики, нормативно-правовому регулированию в области обороны, иные установленные федеральными конституционными законами, федеральными законами, актами Президента Российской Федерации и Правительства Российской Федерации функции в этой области, а также уполномоченным федеральным органом исполнительной власти в сфере управления и распоряжения имуществом Вооруженных Сил Российской

Федерации и подведомственных Министерству обороны Российской Федерации организаций.

В соответствии с Указом Президента Российской Федерации от 16 августа 2004 г. № 1082 «Вопросы Министерства обороны Российской Федерации»[34] Минобороны России осуществляет, в рамках своих полномочий, организацию деятельности по обеспечению информационной безопасности, защите государственной тайны в Вооруженных Силах. организует в установленном порядке в пределах своей компетенции работу по оценке соответствия вооружения и военной техники, проводит по сертификацию средств защиты информации, стандартизацию оборонной продукции и каталогизацию предметов снабжения и др..

Структурным подразделением Министерства обороны, обеспечивающим информационную безопасность можно назвать Восьмое управление Генерального штаба Вооруженных Сил Российской Федерации, которое решает задачи по обеспечению МО РФ необходимой информацией для выполнения текущих задач по управлению ВС РФ. Обеспечивает защиту информации, составляющей государственную тайну. Под руководством Управления созданы подразделения и службы, осуществляющие лицензирование и сертификацию средств защиты информации воинских частей РФ, шифрования радиолиний[35]. Восьмое управление также обеспечивает безопасность ПДн при их обработке в информационных системах Министерства обороны Российской Федерации[36].

Служба внешней разведки Российской Федерации (СВР РФ) организовывает и обеспечивает в пределах своей компетенции защиту государственной тайны в учреждениях Российской Федерации, находящихся за пределами территории Российской Федерации, определяет порядок осуществления физической и инженерно-технической защиты указанных учреждений, мероприятий по

[34] Вопросы Министерства обороны Российской Федерации: указ Президента РФ от 16.08.2004 г. N 1082: по сост. на 27 марта 2017 // Собрание законодательства РФ. – 2004. – N 34. – Ст. 3538.

[35] Восьмое управление Генерального штаба Вооруженных Сил Российской Федерации [Электронный ресурс] // Минобороны России: сайт. – URL: http://structure.mil.ru/structure/ministry_of_defence/details.htm?id=11159@egOrganization (дата обращения 11.04.2017 г.).

[36] Об утверждении Положения об обработке персональных данных в центральном аппарате Министерства обороны Российской Федерации: приказ Министра обороны РФ от 16.06.2012 г. N 1500: по сост. на 23 апреля 2017 г. // Российская газета. – N 227. – 2012.

предотвращению утечки по техническим каналам сведений, составляющих государственную тайну. Обеспечивает безопасность командированных за пределы территории Российской Федерации граждан Российской Федерации, имеющих по роду своей деятельности допуск к сведениям, составляющим государственную тайну, и находящихся с ними членов их семей.

Для достижения целей деятельности СВР РФ может при собственном лицензировании и сертификации разрабатывать (за исключением криптографических средств защиты), а также приобретать, создавать и эксплуатировать информационные системы, системы связи и передачи данных, а также средства защиты информации от утечки по техническим каналам[37].

Федеральная служба безопасности Российской Федерации (ФСБ России) – федеральный орган исполнительной власти, в пределах своих полномочий осуществляющим государственное управление в области обеспечения безопасности Российской Федерации, борьбы с терроризмом, защиты и охраны государственной границы Российской, охраны внутренних морских вод, территориального моря, исключительной экономической зоны, континентального шельфа Российской Федерации и их природных ресурсов, обеспечивающим информационную безопасность Российской Федерации и непосредственно реализующим основные направления деятельности органов федеральной службы безопасности, определенные законодательством Российской Федерации, а также координирующим контрразведывательную деятельность федеральных органов исполнительной власти, имеющих право на ее осуществление[38].

Одним из основных направлений деятельности ФСБ является обеспечение информационной безопасности страны.

ФСБ России осуществляет деятельность по организации и выявлению, предупреждению и пресечению разведывательной и иной деятельности специальных служб и организаций иностранных государств, отдельных лиц,

---

[37] О внешней разведке: федеральный закон от 10.01.1996 г. N 5-ФЗ: по сост. на 24 апреля 2017 г. // Собрание законодательства РФ. – 1996. – N 3. – Ст. 143.

[38] Вопросы Федеральной службы безопасности Российской Федерации: указ Президента РФ от 11.08.2003 г. N 960: по сост. на 17 апреля 2017 г. // Собрание законодательства РФ. – 2003. – N 33. – Ст. 3254.

направленной на нанесение ущерба безопасности Российской Федерации. В пределах своих полномочий обеспечивает защиту государственной тайны, и противодействие иностранным организациям, осуществляющим техническую разведку. Обеспечивает криптографическую и инженерно-техническую безопасность информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи в Российской Федерации и ее учреждениях за рубежом. В пределах своих полномочий формирует и реализует государственную и научно-техническую политику в области обеспечения информационной безопасности страны. Организовывает и проводит научные исследования по проблемам, связанным с обеспечением безопасности личности, общества и государства. Проводит контрразведывательную деятельность. Определяет порядок осуществления органами безопасности проникновения в специальные службы и организации иностранных государств и других контрразведывательных мероприятий, а также использования негласных методов и средств при их реализации. Выполняет мероприятия по сбору, хранению, обработке и использованию документированной информации ограниченного доступа для обеспечения контрразведывательной, разведывательной, оперативно-разыскной и иной деятельности, отнесенной федеральным законодательством к компетенции органов безопасности. Разрабатывает и использует информационные системы, средства защиты информации, в том числе средства криптографической защиты, а также системы связи и передачи данных[39].

ФСБ России для осуществления своей деятельности может разрабатывать и эксплуатировать без лицензирования системы связи, информационные системы и системы передачи данных, а также средства криптографической защиты информации.

При обеспечении информационной безопасности государства ФСБ России формирует и реализует государственную и научно-техническую политику в области обеспечения информационной безопасности, в том числе с использованием

[39] Собрание законодательства РФ. – 2003. – N 33. – Ст. 3254.

инженерно-технических и криптографических средств. Обеспечивает криптографическими и инженерно-техническими методами безопасности информационно-телекоммуникационные системы, сети связи специального назначения и иные сети связи, обеспечивающие передачу шифрованной информации, в Российской Федерации и ее учреждениях, находящихся за пределами Российской Федерации[40].

Федеральная служба охраны Российской Федерации (ФСО России) – федеральный орган исполнительной власти в области государственной охраны, осуществляет функции по выработке и реализации государственной политики, нормативно-правовому регулированию, контролю и надзору в сфере государственной охраны, связи для нужд органов государственной, а также функции по информационно-технологическому и информационно-аналитическому обеспечению деятельности Президента Российской Федерации, Правительства Российской Федерации, иных государственных органов[41].

ФСО России в пределах своих полномочий участвует в обеспечении информационной безопасности Российской Федерации. Обеспечивает организацию и функционирование федеральных информационных систем, находящихся во владении или пользовании органов государственной охраны. Организовывает и выполняет шифровальную деятельность в органах государственной охраны.

Совместно с ФСБ России проводит работу по защите информации в сетях связи специального назначения, федеральных информационных системах для специального информационного обеспечения государственных органов и на охраняемых объектах, мероприятия по выявлению электронных устройств, предназначенных для негласного получения информации, а также специальные исследования технических средств и оборудования, находящихся в ведении ФСО России. Обеспечивает надежное функционирование и информационную безопасность федеральных информационных систем для специального

---

[40] О Федеральной службе безопасности: федеральный закон от 03.04.1995 г. N 40-ФЗ: по сост. на 15 апреля 2017 г. // Собрание законодательства РФ. – 1995. – N 15. – Ст. 1269.

[41] Вопросы Федеральной службы охраны Российской Федерации: указ Президента РФ от 07.08.2004 г. N 1013: по сост. на 19 апреля 2017 г. // Собрание законодательства РФ. – 2004. – N 32. – Ст. 3314.

информационного обеспечения государственных органов, а также разрабатывает и эксплуатирует такие системы. Организует деятельность по созданию и разработке средств защиты информации, в том числе системы специальных технических средств, а также в разработке нормативно-технической документации по вопросам защиты информации в сетях связи специального назначения и федеральных информационных системах для специального информационного обеспечения государственных органов. Проводит мероприятия по организации и обеспечению функционирования, совершенствования и информационной безопасности сетей связи специального назначения в интересах находящихся за рубежом представителей государственных органов, а также дипломатических представительств и консульских учреждений Российской Федерации[42].

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) – федеральный орган исполнительной власти, осуществляющий реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по обеспечению информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере, в том числе в функционирующих в составе критически важных объектов Российской Федерации информационных системах и телекоммуникационных сетях, деструктивные информационные воздействия на которые могут привести к значительным негативным последствиям. Осуществляет деятельность по противодействию иностранным техническим разведкам на территории Российской Федерации. Обеспечивает защиту государственной тайны и иной информации с ограниченным доступом, предотвращает ее утечку по техническим каналам, несанкционированного доступа, специальных воздействий на носители информации в целях ее добывания, искажения, уничтожения и блокирования доступа к ней на территории Российской Федерации. Проводит мероприятия по разработке, эксплуатации и утилизации

[42] О государственной охране: федеральный закон от 27.05.1996 г. N 57-ФЗ: по сост. на 24 апреля 2017 г. // Собрание законодательства РФ. – 1996. – N 22. – Ст. 2594.

неинформационных излучающих систем, комплексов и устройств, а также их защиту. Обеспечивает безопасность информации в ключевых системах информационной инфраструктуры, противодействие техническим разведкам и техническую защиту информации. Осуществляет самостоятельно нормативно-правовое регулирование вопросов связанных с обеспечением безопасности информации в ключевых системах информационной инфраструктуры, противодействием техническим разведкам, технической защиты информации; размещения и использования иностранных технических средств наблюдения и контроля в ходе реализации международных договоров Российской Федерации, иных программ и проектов на территории Российской Федерации, на континентальном шельфе и в исключительной экономической зоне Российской Федерации.

Осуществляет лицензирование деятельности по проведению мероприятий или оказанию услуг в области защиты государственной тайны, по созданию средств защиты информации, составляющей государственную тайну, по технической защите конфиденциальной информации, по разработке и производству средств защиты конфиденциальной информации. Проводит государственный и межведомственный контроль за обеспечением защиты государственной тайны, контроль за соблюдением лицензионных требований и условий, а также рассмотрение дел об административных правонарушениях.

Проводит специальные экспертизы, совместно с ФСБ России по допуску организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, а также принимает участие в проведении государственной аттестации руководителей организаций, ответственных за защиту указанных сведений[43].

Федеральным органом исполнительной власти, осуществляющим функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, а также специальные функции в сфере

[43] Вопросы Федеральной службы по техническому и экспортному контролю: указ Президента РФ от 16.08.2004 г. N 1085: по сост. на 26 апреля 2017 г. // Собрание законодательства РФ. – 2004. – N 34. – Ст. 3541.

обеспечения федеральной фельдъегерской связи в Российской Федерации является Государственная фельдъегерская служба Российской Федерации (ГФС России).

Данная служба обеспечивает доставку в города федерального значения, столицы и административные центры субъектов Российской Федерации и обратно, столицы государств - участников Соглашения о Межправительственной фельдъегерской связи отправлений особой важности, совершенно секретных, секретных и иных служебных отправлений, обеспечивает доставку корреспонденции органов СНГ.

В пределах своей компетенции обеспечивает защиту государственной и иной охраняемой законом тайны, а также по согласованию с ФСБ России принимает меры, связанные с допуском сотрудников центрального аппарата ГФС России и ее территориальных органов к сведениям, составляющим государственную тайну.

Занимается разработкой и эксплуатацией информационных систем, систем связи и систем передачи данных, а также средств защиты информации. Обеспечивает контроль уровня защищенности информации в ГФС России и ее территориальных органах[44].

Центральный Банк России в сфере обеспечения информационной безопасности банковской системы разрабатывает и утверждает стандарты и рекомендации. Например, такие как СТО БР ИББС-1.3-2016[45], СТО БР ИББС-1.0-2014[46], СТО БР ИББС-1.2-2014[47], РС БР ИББС-2.0-2007[48] и другие.

---

[44] Вопросы Государственной фельдъегерской службы Российской Федерации: указ Президента РФ от 07.04.2014 г. N 213: по сост. на 27 апреля 2017 г. // Собрание законодательства РФ. – 2014. – N 15. – Ст. 1726.

[45] Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств «СТО БР ИББС-1.3-2016»: Стандарт Банка России от 30.11.2016 г. N ОД-4234: по сост. на 27 апреля 2017 г. // Вестник Банка России. – N 107. – 2016.

[46] Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения СТО БР ИББС-1.0-2014: Стандарт Банка России от 17.05.2014 г. N Р-399: по сост. на 23 мая 2017 г. // Вестник Банка России. – N 48-49. – 2014.

[47] Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014 «СТО БР ИББС-1.2-2014»: Стандарт Банка России от 17.05.2014 г. N Р-399: по сост. на 27апреля 2017 г. // Вестник Банка России. – N 48-49. – 2014.

[48] Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0» РС БР ИББС-2.0-2007: приняты и

Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере СМИ, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки ПДн требованиям законодательства Российской Федерации в области ПДн, а также функции по организации деятельности радиочастотной службы – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)[49].

В пределах своей компетенции проводит аккредитацию экспертов и экспертных организаций для проведения экспертизы информационной продукции в целях обеспечения информационной безопасности детей.

Осуществляет контроль и надзор в сфере защиты детей от информации, причиняющей вред их здоровью и развитию, - за соблюдением требований законодательства Российской Федерации в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию, к производству и выпуску СМИ, вещанию телеканалов, радиоканалов, телепрограмм и радиопрограмм, а также к распространению информации посредством информационно-телекоммуникационных сетей (в том числе сети «Интернет») и сетей подвижной радиотелефонной связи.

Ведет реестр операторов, осуществляющих обработку ПДн. Также ведет и формирует Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено[50], в который в соответствии с правилами вносятся интернет ресурсы с запрещенной на территории Российской Федерации информацией.

введены в действие Распоряжением Банка России от 28.04.2007 г. N Р-348: по сост. на 27 апреля 2017 г. // Вестник Банка России. – N 29. –2007.

[49] О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций: постановление Правительства РФ от 16.03.2009 г. N 228: по сост. на 27 апреля 2017 г. // Собрание законодательства РФ. – 2009. – N 12. – Ст. 1431.

[50] О единой автоматизированной информационной системе Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать

К такой информации[51] относятся:

Материалы с порнографическими изображениями несовершеннолетних или объявления о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;

Информация, о способах и методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств, веществ и их прекурсоров, а также о способах и местах культивирования наркосодержащих растений;

Информации о способах совершения самоубийства, а также призывов к совершению самоубийства.

Самостоятельным структурным подразделением центрального аппарата Министерства внутренних дел Российской Федерации является Департамент информационных технологий, связи и защиты информации Министерства внутренних дел Российской Федерации[52], который в пределах своей компетенции обеспечивает и осуществляет функции Министерства по выработке и реализации государственной политики, нормативному правовому регулированию в области совершенствования информационных и телекоммуникационных технологий, автоматизированных информационных систем, систем и средств связи, радио- и радиотехнического контроля, обеспечения электромагнитной совместимости

сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено: постановление Правительства РФ от 26.10. 2012 г. N 1101: по сост. на 25 апреля 2017 г. // Собрание законодательства РФ. – 2012. – N 44. – Ст. 6044.

[51] Об утверждении критериев оценки материалов и (или) информации, необходимых для принятия решений Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, Федеральной службой Российской Федерации по контролю за оборотом наркотиков, Федеральной службой по надзору в сфере защиты прав потребителей и благополучия человека о включении доменных имен и (или) указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет», а также сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие запрещенную информацию, в единую автоматизированную информационную систему «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» приказ Роскомнадзора N 1022, ФСКН России N 368, Роспотребнадзора N 666 от 11.09.2013 г.: по сост. на 28 апреля 2017 г. // Российская газета. – N 262. – 2013.

[52] Положение о Департаменте информационных технологий, связи и защиты информации МВД России: приказ N 681, утверждено приказом МВД России от 16 июня 2011 г. [Электронный ресурс]. URL: https://мвд.рф/mvd/structure1/Departamenti/Departament_informacionnih_tehnologij_sv/Polozhenie/ (дата обращения 27.04. 2017 г.).

радиоэлектронных средств, противодействия техническим разведкам, технической (в том числе криптографической) защиты информации, радиоэлектронной борьбы, использования электронной подписи, формирования и ведения информационных ресурсов, межведомственного информационного взаимодействия, реализации государственных и ведомственных программ в области информатизации, навигационно-мониторинговых систем органов внутренних дел, организаций и подразделений, созданных для выполнения задач и осуществления полномочий, возложенных на МВД России, внутренних войск МВД России. Также осуществляет защиту государственной тайны и информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, проводит оценку и анализирует состояния информатизации, связи и защиты информации в системе Министерства, определяет приоритетные направления совершенствования. Производит прогноз развития информационных технологий, связи и защиты информации, разработку предложений руководству МВД России по их совершенствованию.

В структуре МВД также можно выделить Управление «К» МВД России, основной деятельностью которого является борьба с преступностью в сфере компьютерной информации, а также в информационно- телекоммуникационных сетях, включая сеть Интернет. Управление борется с незаконным оборотом радиоэлектронных и специальных технических средств. Выявляет и пресекает факты нарушения авторских и смежных прав в сфере информационных технологий. Борется с международными преступлениями в сфере информационных технологий. Осуществляет сотрудничество с зарубежными государствами в целях борьбы с преступлениями, совершаемыми с использованием информационных технологий[53].

Таким образом субъектами, обеспечивающими информационную безопасность личности, общества и государства в Российской Федерации являются:

Президент Российской Федерации;

---

[53] Управление «К» МВД России [Электронный ресурс] // МВД России: сайт. – URL: https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii (дата обращения 08.04.2017 г.).

Совет Федерации и Государственная Дума (Комитет Государственной Думы по безопасности и противодействию коррупции);

Правительство Российской Федерации;

Совет безопасности Российской Федерации (Межведомственная комиссия Совета Безопасности Российской Федерации);

Министерство обороны Российской Федерации (Восьмое управление Генерального штаба Вооруженных Сил Российской Федерации);

Служба внешней разведки Российской Федерации;

Федеральная служба безопасности Российской Федерации;

Федеральная служба охраны Российской Федерации;

Федеральная служба по техническому и экспортному контролю;

Государственная фельдъегерская служба Российской Федерации;

Центральный Банк России;

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций;

Министерство внутренних дел Российской Федерации (Департамент информационных технологий, связи и защиты информации Министерства внутренних дел Российской Федерации. Управление «К» МВД России).

1.3 Зарубежный опыт обеспечения информационной безопасности

Для обеспечения национальной безопасности, а также для удовлетворения своих амбиций США стремятся к глобальному доминированию в военной, экономической, научной, информационной и других областях. Соединенные Штаты хотят сохранить статус единственной сверхдержавы. Для достижения этой цели им также необходимо обеспечить превосходство и в информационной безопасности.

Конституция США, принятая 17 сентября 1787 года в Филадельфии прямо не закрепляет положения об информационной безопасности, однако некоторые положения содержатся в принятых поправках 15 декабря 1791 года.

Так в первой поправке закреплено право на свободу религии, свободу слова, свободу печати, свободу собраний и право на петицию. Данная поправка также содержит, что Конгрессу запрещено издавать законы, которые могут ограничить эти права. Четвертая поправка содержит положения на неприкосновенность частной жизни. Данная поправка защищает граждан от необоснованных обысков самих себя или имущества и задержаний со стороны государственных органов. Обыском считается как обыск дома или автомобиля, так и требования сотрудниками полиции, например, проведения анализа крови[54].

Рассмотрим нормативно-правовые акты, регулирующие информационную безопасность США.

Федеральным законом Соединенных Штатов, регламентирующим сбор, обслуживание, использование и распространение личной информации о гражданах, которая хранится в системах записей (базах данных) федеральных агентств, является Закон о конфиденциальности (Privacy Act) принятый 31 декабря 1974 года.

Система записей представляет собой базу данных, которая хранится в том или ином органе власти, агентстве или организации. В этих системах записей хранятся персональные данные граждан, по которой можно идентифицировать личность. Закон о неприкосновенности частной жизни требует, чтобы агентства публично уведомляли о своих системах записей путем публикации в Федеральном регистре. Закон о неприкосновенности частной жизни запрещает разглашение информации из системы записей без письменного согласия субъекта, если раскрытие не осуществляется в соответствии с одним из двенадцати предусмотренных законом исключений.

Закон также предоставляет гражданам возможность для получения доступа к их собственным учетным записям и внесения в них поправок. Закон устанавливает требования к ведению учета в ведомстве. Кроме того, с предоставленным гражданам правом пересматривать свои персональные данные, внесенные в базу, они также

---

[54] Constitution of the United States [Электронный ресурс] // United States Senate: сайт. – URL: https://www.senate.gov/civics/constitution_item/constitution (дата обращения 25.04.2017 г.).

могут выяснить, предоставлялись ли их персональные данные по запросу другому ведомству[55].

Информация может быть предоставлена только – должностным лицам и сотрудникам агентства, которое ведет учет при исполнении своих обязанностей; в Бюро переписи для целей планирования или проведения переписи или исследования и связанной с ней деятельности; гражданину, который предоставил агентству заблаговременно письменное подтверждение того, что запись будет использоваться исключительно в качестве статистического исследования или отчета, и запись должна быть передана в форме, не поддающейся индивидуальной идентификации; в Национальное управление архивов и документации в качестве записи, которая имеет достаточную историческую или другую ценность для обеспечения ее сохранения правительством Соединенных Штатов или для оценки Архивариусом Соединенных Штатов или назначенным архивистом для определения того, будет ли запись имеет такое значение; в другое учреждение или под юрисдикцию какой-либо правительственной юрисдикции в Соединенных Штатах или под их контролем за деятельностью в области гражданского или уголовного права, если деятельность санкционирована законом и если руководитель учреждения или орган совершил письменный запрос в агентство, которое ведет запись с указанием конкретной цели для предоставления записи; в любую Палату Конгресса, любой комитет или подкомитет Конгресса; по решению суда и т. д[56]..

Закон о банковской тайне принятый в 1970 года содержит требования к финансовым учреждениям в Соединенных Штатах Америки осуществлять защиту информации о клиентах.

Также закон обязует банки помогать государственным учреждениям США выявлении и предотвращении отмывания денег. В частности, в соответствии с этим законом финансовые учреждения должны вести учет покупок и оборота денежных

---

[55] Privacy Act 1974 [Электронный ресурс] // U.S. Government Publishing Office: сайт. – URL: https://www.gpo.gov/fdsys/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf (дата обращения 20.04.2017 г.).

[56] Government organization and employees [Электронный ресурс] // U.S. Government Publishing Office: сайт. – URL: https://www.gpo.gov/fdsys/pkg/USCODE-2010-title5/html/USCODE-2010-title5-partI-chap5-subchapII-sec552a.htm (дата обращения 19.04.2017 г.).

средств клиентов и сообщать в органы власти, если сумма покупок превышает 10 тыс. долларов в день. Такой оборот денежных средств считается подозрительной деятельностью, которая может означать отмывание денег, уклонение от уплаты налогов, или другие преступления. При этом банку запрещено сообщать клиенту о том, что по его покупках или обороте денежных средств был передан отчет в соответствующие органы. Такой отчет содержит номер банковского счета, ФИО клиента, его адрес и номер социального страхования, а также информацию о транзакциях, которые вызвали подозрение[57].

Закон о конфиденциальности электронных коммуникаций был принят Конгрессом Соединенных Штатов 21 октября 1986 года для ограничения Правительства на прослушивание телефонных разговоров, включая передачу электронных данных с помощью компьютера

Под «электронной коммуникацией» понимается любая передача знаков, сигналов, писем, изображений, звуков, данных или сведений любого характера, передаваемых полностью или частично через проводные сети, радио, электромагнитной, фотоэлектронной или фотооптической системой за исключением телефонного или устного общения; связи, осуществляемой с помощью пейджингового устройства только для тональных сигналов; информации о передаче данных, хранящихся финансовым учреждением в своей системе, используемой для электронного хранения и перевода денежных средств.

Глава первая закона содержит положения по защите проводных, устных и электронных сообщений во время доставки. Он устанавливает требования к операторам, осуществляющим доставку сообщений по защите данных. Во второй главе содержатся положения по защите информации, которая хранится в электронном виде, в первую очередь на компьютерах. Глава третья содержит

[57] The Bank Secrecy Act of 1970 [Электронный ресурс] // U.S. Government Publishing Office: сайт. – URL: https://www.gpo.gov/fdsys/pkg/STATUTE-84/pdf/STATUTE-84-Pg1114-2.pdf (дата обращения 13.04.2017 г.).

положения о запрете использования специальных средств и инструментов для сбора и перехвата данных без судебного распоряжения[58].

Закон об компьютерном мошенничестве и злоупотреблениях (CFAA) был принят Конгрессом в 1986 году. Закон в основном регулирует защиту компьютеров и систем федерального правительства и финансовых учреждений, а также если преступление является межгосударственным. Содержатся положения о запрете на распространение вредоносного кода и атак на системы. Конгресс также включил в CFAA положение, запрещающее торговлю паролями и подобными ресурсами[59].

В Закон неоднократно вносились поправки - в 1989, 1994, 1996 годах, в 2001 году в соответствии с Законом США о свободе вероисповедания в 2002 году и в 2008 году - Законом о защите личных данных. В январе 2015 года Барак Обама предложил расширить CFAA в связи с Модернизацией правоохранительных органов для борьбы с киберпреступностью[60].

Федеральный Закон о защите конфиденциальности детей в Интернете, вступивший в силу 21 апреля 2000 года. Распространяется на онлайн-сбор персональной информации о детях младше 13 лет, находящихся под юрисдикцией США.

В законе подробно описывается, что оператор веб-сайта должен осуществлять политику конфиденциальности, иметь согласие со стороны родителей или опекунов о сборе и обработке информации. Также закреплены обязанности оператора по защите информации в отношении детей, включая ограничения на информацию рекламного характера, которую могут увидеть несовершеннолетние пользователи[61].

---

[58] The Electronic Communications Privacy Act of 1986 (ECPA) [Электронный ресурс] // U.S. Government Publishing Office: сайт. – URL: https://www.gpo.gov/fdsys/pkg/STATUTE-100/pdf/STATUTE-100-Pg1848.pdf (дата обращения 18.04.2017 г.).

[59] Computer Fraud and Abuse Act of 1986 [Электронный ресурс] // Library of Congress: сайт. – URL: https://www.congress.gov/bill/99th-congress/house-bill/4718/text (дата обращения 11.04.2017 г.).

[60] Securing cyberspace - President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts [Электронный ресурс] // The White House President Barack Obama https://obamawhitehouse.archives.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat (дата обращения 09.04.2017 г.).

[61] The Children's Online Privacy Protection Act of 1998 (COPPA) [Электронный ресурс] // U.S. Government Publishing Office: сайт. – URL: https://www.gpo.gov/fdsys/pkg/PLAW-105publ277/html/PLAW-105publ277.htm (дата обращения 19.04.2017 г.).

Хотя дети в возрасте до 13 лет могут вполне легально предоставлять личную информацию с разрешения своих родителей, многие веб-сайты, особенно сайты социальных сетей, запрещают несовершеннолетним детям использовать их услуги. В целом это связано из-за сложностей, связанных с соблюдением закона[62].

В США наиболее часто употребляется термин «кибербезопасность» (cybersecurity), который относится в основном к обеспечению безопасности информационно-телекоммуникационной сети Интернет, а в РФ для этого используется обобщающий термин «информационная безопасность»[63].

Три закона закрепляют основные правила кибербезопасности - Закон о медицинском страховании и ответственности (Health Insurance Portability and Accountability Act)[64] принятый в 1996 году, Закон о модернизации финансовых услуг (Financial Services Modernization Act)[65] 1999 года и Закон о национальной безопасности (The Homeland Security Act) 2002 года, в который включен Федеральный закон об управлении информационной безопасностью (The Federal Information Security Management Act. FISMA)[66].

Эти три нормативных акта предписывают организациям здравоохранения, финансовым учреждениям и федеральным агентствам защищать свои системы и информацию. Например, Закон FISMA, который применяется ко всем государственным учреждениям, «требует разработку и реализацию обязательной политики, принципов и стандартов информационной безопасности». Однако в этих положениях не указывается, какие меры по обеспечению кибербезопасности должны быть реализованы и которые требуют именно «разумного» уровня

---

[62] Letting Your Kids Play in the Social Media Sandbox [Электронный ресурс] // The New York Times's: сайт. – URL: https://www.nytimes.com/2015/02/19/style/letting-your-kids-play-in-the-social-media-sandbox.html?_r=0 (дата обращения 23.04.2017 г.).

[63] Булавин А.В. О подходах США и Китая к обеспечению кибербезопасности // Общество: политика, экономика, право. 2014. №1. С. 28.

[64] Health Insurance Portability and Accountability Act of 1996 [Электронный ресурс] // U.S. Government Publishing Office: сайт. – URL: https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm (дата обращения 23.04.2017 г.).

[65] Financial Services Modernization Act of 1999 [Электронный ресурс] // U.S. Government Publishing Office: сайт. – URL: https://www.gpo.gov/fdsys/pkg/STATUTE-113/pdf/STATUTE-113-Pg1338.pdf (дата обращения 30.04.2017 г.).

[66] The Federal Information Security Management Act of 2002 [Электронный ресурс] // U.S. Government Publishing Office: сайт. – URL: http://www.gpo.gov/fdsys/pkg/STATUTE-116/pdf/STATUTE-116-Pg2899.pdf (дата обращения 27.04.2017 г.).

безопасности. Смутные формулировки этих положений оставляют много вопросов в толковании.

После трагических событий 11 сентября 2001 года стало понятно, что необходимо проводить модернизацию и обновление политики в сфере национальной безопасности, а также и в обеспечении информационной безопасности страны.

Закон о предотвращении и наказании террористических актов в Соединенных Штатах и во всем мире, совершенствование инструментов расследования в правоохранительных органах (USA PATRIOT) [67] этот закон был подписан президентом Джорджем Бушем 26 октября 2001 года.

Глава 8 содержит положения о борьбе с терроризмом, в том числе и с кибертерроризмом. Кибертерроризм рассматривается по-разному. Под ним понимаются действия, с помощью которых кто-либо наносит ущерб физическому и психическому здоровью граждан, склоняя к причинению вреда себе, либо получают несанкционированный доступ к защищенному компьютеру, а также действия, которые могут вызвать угрозу общественной безопасности. Запрещено также вымогательство через информационно-телекоммуникационные сети. Наказание предусмотрено как в виде штрафа, так и лишение свободы.

26 мая 2011 года президент США Барак Обама подписал Закон о продлении срока действия USA PATRIOT на четыре года трех ключевых положений закона: прослушивание телефонных разговоров, анализ деловых переписок и наблюдение за лицами, подозреваемые в террористической деятельности, не связанной с террористическими группами[68].

После отсутствия одобрения Конгресса части Патриотического акта истекли 1 июня 2015 года. С принятием Закона США о свободе 2 июня 2015 года истекшие части были восстановлены и возобновлены до 2019 года. Однако были внесены

---

[67] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001[Электронный ресурс] // U.S. Government Publishing Office: сайт. – URL: https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf (дата обращения 28.04.2017 г.).

[68] Obama Signs Last-Minute Patriot Act Extension [Электронный ресурс] // Fox News Politics: сайт. – URL: http://www.foxnews.com/politics/2011/05/27/senate-clearing-way-extend-patriot-act.html (дата обращения 18.04.2017 г.).

поправки, в соответствии с которыми Агентство национальной безопасности прекращает сбор данных по прослушиванию телефонных линий. Вместо этого телефонные компании будут хранить данные, и АНБ может получить информацию о конкретных лицах с разрешения федерального суда[69].

В 2002 году была принята новая стратегия национальной безопасности, в которой США заявили, что международный терроризм является основной угрозой национальной безопасности государства.

Обеспечение информационного контроля стало необходимым условием для предупреждения и предотвращения угроз. Информационный контроль включает в себя:

1) Использование технологий для получения информации об угрозах и потенциальных противниках.
2) Предотвращение возможности получения информации противником о собственных средствах и силах.
3) Надежная защита собственной инфраструктуры и информации[70].

В стратегии национальной безопасности США, принятой 2002 году, ключевым стал принцип «превентивных действий», т.е. угрозы не должны перерастать в прямое нападение на государство, а должны ликвидироваться на начальном этапе. Потенциальные угрозы уничтожались также и военными действиями. Соответственно, чтобы воплотить это в жизнь необходимо располагать огромным массивом разведывательной информации и осуществлять в реальном времени постоянный сбор и анализ подобной информации.

Закон о защите конфиденциальной информации и статистической эффективности (CIPSEA) - это федеральный закон Соединенных Штатов, принятый в 2002 году в качестве раздела V Закона об электронном правительстве.

---

[69] Senate approves USA Freedom Act [Электронный ресурс] // USA today: сайт. – URL: https://www.usatoday.com/story/news/politics/2015/06/02/patriot-act-usa-freedom-act-senate-vote/28345747/ (дата обращения 07.04.2017 г.).

[70] Шариков П.А. Политика США в области информационной безопасности: дис. ... канд. полит. наук: 23.00.04 / П.А Шариков. М, 2009. С. 113.

CIPSEA устанавливает единые гарантии конфиденциальности информации, собираемой статистическими агентствами, и обеспечивает возможность обмена данными между Бюро статистики труда, Бюро экономического анализа и Бюро переписи населения. Закон предоставляет агентствам стандартизованные подходы к защите информации от того, чтобы по предоставленным данным нельзя было идентифицировать граждан. Данные респондента используются только в статистических целях. Если гражданин дает письменное согласие, тогда данные могут быть использованы и для других целей[71].

В январе 2008 года президент Джордж Буш в президентской директиве о национальная безопасности 54 и 23 (NSPD-54 / HSPD-23) была учреждена Всеобъемлющая национальная инициатива по кибербезопасности (CNCI)[72]. В этой инициативе излагаются цели по кибербезопасности США и в том числе деятельность органов власти таких как Департамент внутренней безопасности, Управление по вопросам управления и бюджета и Агентство национальной безопасности.

Текущие цели инициативы включают:

–установление линии обороны против современных угроз, повышая уровень осведомленности о сетевых уязвимостях, угрозах и событиях, быстро реагировать на них;

–обеспечение защиты от полного спектра угроз путем усиления возможностей контрразведки США;

–повышение безопасности разработок для ключевых информационных технологий;

–укрепление будущего положения кибербезопасности посредством подготовки кадров и проведения исследований.

---

[71] The Confidential Information Protection and Statistical Efficiency Act of 2002 [Электронный ресурс] // Government library U.S.: сайт. – URL: https://www.eia.gov/cipsea/cipsea.pdf (дата обращения 15.04.2017 г.).

[72] The Comprehensive National Cybersecurity Initiative [Электронный ресурс] // Federation of American Scientists: сайт. – URL: https://fas.org/irp/eprint/cnci.pdf (дата обращения 09.04.2017 г.).

Директива о политике президента 20 (PPD-20)[73] обеспечивает основу для кибербезопасности США, устанавливая принципы и процессы. Подписанная президентом Бараком Обамой в октябре 2012 года, эта директива заменяет собой президентскую директиву Национальной безопасности NSPD-38. Интегрируя кибер-инструменты с инструментами национальной безопасности, эта директива дополняет NSPD-54 / Президентскую директиву HSPD-23 по Национальной Безопасности, также дает возможность правительству США проводить наблюдение посредством мониторинга конфиденциальной информации[74].

Далее рассмотрим основные органы государственной власти США, которые обеспечивают информационную безопасность государства.

Совет национальной безопасности Белого дома[75] является главным совещательным органом, используемым Президентом Соединенных Штатов для рассмотрения вопросов национальной безопасности и внешней политики со старшими советниками по национальной безопасности и должностными лицами Кабинета, входит в состав исполнительной канцелярии президента Соединенных Штаты. С момента своего создания под руководством Гарри С. Трумэна, функции Совета заключались в том, чтобы консультировать и помогать президенту в вопросах национальной безопасности и внешней политики. Совет также выступает в качестве основного рычага президента для координации этой политики между различными правительственными учреждениями. У Совета есть партнеры в Советах национальной безопасности многих других стран.

Управление по надзору за информационной безопасностью (ISOO)[76] несет ответственность перед Президентом за политику и контроль над системой классификации безопасности в масштабах всего государства и Национальной программой промышленной безопасности в США. ISOO является составной частью

---

[73] Presidential Policy Directive 20 (PPD-20) [Электронный ресурс] // Federation of American Scientists: сайт. – URL: https://fas.org/irp/offdocs/ppd/ppd-20.pdf (дата обращения 05.04.2017 г.).

[74] EPIC v. NSA - Cybersecurity Authority [Электронный ресурс] // Electronic Privacy Information Center: сайт. – URL: https://epic.org/foia/nsa/nspd-54/default.html (дата обращения 16.04.2017 г.).

[75] National Security Council [Электронный ресурс] // The White House President Donald J. Trump: сайт. – URL: https://www.whitehouse.gov/nsc/ (дата обращения 14.04.2017 г.).

[76] Information Security Oversight Office (ISOO) [Электронный ресурс] // The U.S. National Archives and Records Administration: сайт. – URL: https://www.archives.gov/isoo (дата обращения 16.05.2017 г.).

Национального управления архивов и документации и получает рекомендации по вопросам политики и программ от Совета национальной безопасности.

Комитет по безопасности телекоммуникаций и информационных систем национальной безопасности (NSTISSC)[77] был создан в соответствии с Директивой национальной безопасности 42 «Национальная политика в области обеспечения безопасности телекоммуникационных и информационных систем национальной безопасности» от 5 июля 1990 года.

NSTISSC проводит обсуждение вопросов политики, устанавливает национальную политику, направления, оперативные процедуры и руководство для информационных систем, управляемых правительством США, его подрядчиками или агентами, которые содержат секретную информацию, осуществляют разведывательную деятельность, включают криптографическую деятельность, связанную с национальной безопасностью, осуществляют командование и контроль над вооруженными силами, включают в себя оборудование, которое является неотъемлемой частью системы информационной безопасности.

Департамент внутренней безопасности Соединенных Штатов (DHS)[78] - это орган власти федерального правительства Соединенных Штатов, в обязанности которого входит обеспечение общественной безопасности, что примерно соответствует внутренним министерствам других стран.

Его основной деятельностью является: борьба с терроризмом, безопасность границ, таможенный контроль и контроль за иммиграцией, кибербезопасность, предупреждение и ликвидация стихийных бедствий. Департамент был создан после нападения 11 сентября 2001года.

Национальная политика безопасности координируется в Белом доме Советом национальной безопасности.

Для обеспечения информационной безопасности осуществляет анализ и уменьшение кибер-угроз и уязвимости в телекоммуникационных системах;

---

[77] National Security Telecommunications and Information Systems Security Committee (NSTISSC) [Электронный ресурс] // Committee national security systems: сайт. – URL: https://www.cnss.gov/ (дата обращения 03.05.2017 г.).

[78] Cybersecurity [Электронный ресурс] // United States Department of Homeland Security: сайт. – URL: https://www.dhs.gov/topic/cybersecurity (дата обращения 13.05.2017 г.).

уведомляет о существующих угрозах; а также обеспечивает безопасность компьютерных сетей.

Национальный центр кибербезопасности (NCSC) является подразделением Департамента внутренней безопасности США (DHS), созданным в марте 2008 года, и основывается на требованиях Президентской директивы по национальной безопасности 54 / Национальная политика в области безопасности на дому 23 (NSPD-54 / HSPD -23), NCSC поручено защищать коммуникационные сети правительства США. Центр обеспечивает защиту и обмен информации в системах, принадлежащих АНБ, ФБР, Министерство обороны и Департамента внутренней безопасности.

Управление кибербезопасности и коммуникаций (CS&C) в рамках Национального управления по защите программ отвечает за повышение безопасности, отказоустойчивости и надежности кибер-коммуникационной инфраструктуры страны. CS&C работает над предотвращением или минимизацией сбоев в работе критически важной информационной инфраструктуры, чтобы защитить общественность, экономику и правительственные службы. CS&C ведет работу по защите федерального домена- .gov гражданских правительственных сетей и частного сектора домена- .com. Кроме того, обеспечивает круглосуточный кибер-мониторинг, реагирует на инциденты.

Национальный отдел кибербезопасности (NCSD) является подразделением Управления кибербезопасности и коммуникаций в рамках Управления национальной безопасности и программ Департамента внутренней безопасности Соединенных Штатов. Миссия отдела заключается в сотрудничестве с частным сектором, правительством и заинтересованными лицами разведки для проведения оценки рисков и смягчения уязвимостей и угроз для активов и деятельности в области информационных технологий, влияющих на функционирование критически важных кибер-инфраструктур гражданского, правительственного и частного сектора. NCSD также обеспечивает анализ кибер-угроз и уязвимости, раннее предупреждение и помощь в реагировании на инциденты. NCSD выполняет

большую часть обязанностей Департамента внутренней безопасности США в рамках Всеобъемлющей национальной инициативы в области кибербезопасности.

Кибер-командование Соединенных Штатов (USCYBERCOM) является подразделением вооруженных сил, подчиненных Стратегическому командованию Соединенных Штатов. Эта структура централизует управление операциями в киберпространстве, организует существующие кибер-ресурсы и синхронизирует защиту военных сетей США. Для работы используются сети АНБ и возглавляется директором Агентства национальной безопасности. Первоначально оно было создано с оборонительной миссией, однако в настоящее время его все чаще рассматривают как наступательную силу[79].

Совет по надзору за соблюдением конфиденциальности и гражданских прав (PCLOB)[80] является независимым агентством в исполнительной ветви власти, учрежден 11 сентября 2007 года.

Миссия PCLOB - обеспечить, чтобы усилия федерального правительства по предотвращению терроризма были сбалансированы с защитой частной жизни и гражданских прав.

Совет проводит анализ действий, предпринимаемых государственной властью для защиты нации от терроризма. Обеспечивает надлежащее рассмотрение вопросов гражданских прав в разработке и реализации законов, положений и политики, связанных с усилиями по защите нации от терроризма.

Агентство национальной безопасности (англ. National Security Agency, NSA) по своей сути является военной разведкой, которая входит в состав Министерства обороны Соединенных Штатов. АНБ осуществляет глобальный мониторинг, сбор и обработку информации для целей внешней разведки и контрразведки с помощью Signals intelligence (SIGINT) дословный перевод с английского «интеллектуальные сигналы».

---

[79] Obama to be urged to split cyberwar command from NSA [Электронный ресурс] // The Washington Post: сайт. – URL: https://www.washingtonpost.com/world/national-security/obama-to-be-urged-to-split-cyberwar-command-from-the-nsa/2016/09/12/0ad09a22-788f-11e6-ac8e-cf8e0dd91dc7_story.html?utm_term=.bdd8147f3173 (дата обращения 12.05.2017 г.).

[80] About the Board [Электронный ресурс] // Privacy and Civil Liberties Oversight Board: сайт. – URL: https://www.pclob.gov/about-us.html (дата обращения 11.05.2017 г.).

SIGINT – это система технических средств по сбору разведывательных данных путем перехвата сигналов, будь то общение между людьми через телекоммуникационные системы или электронные сигналы, не используемые непосредственно в связи. Поскольку секретная информация всегда зашифровывается, в свою очередь, анализ данных включает использование криптоанализа для расшифровки сообщений, анализ трафика представляет собой перехваченную информацию отправителя, а также кому адресовано сообщение и способ передачи этих данных.

На официальном сайте АНБ заявлено, что миссией агентства является получение преимущества для решения вопросов, связанных с национальными интересами страны и их союзников при любых обстоятельствах[81].

В составе АНБ также осуществляет свою деятельность Центральная служба безопасности (CSS), которая занимается сбором, перехватом и анализом информации в области разведки, криптологии и данных на тактическом уровне. Обеспечивает защиту передачи данных между Правительством США и военным командованием для решения важнейших вопросов в области обороны и реализации целей национальной и тактической разведки.

Также CSS координирует и разрабатывает политику и планы реализации миссий по анализу данных и обеспечению безопасности информации.

CSS была утверждена президентской директивой в 1972 году. Директор АНБ также возглавляет эту службу[82].

АНБ одновременно обеспечивает защиту коммуникационных и информационных систем правительства США от проникновения и сетевых атак. Многие программы АНБ основаны на «пассивном» электронном сборе информации, агентство имеет право выполнять свою миссию с помощью активных средств, среди которых физическое подслушивание электронные систем объектов, которые предположительно могут угрожать национальной безопасности.

---

[81] Mission & Strategy NSA [Электронный ресурс] // National Security Agency: сайт. – URL: https://www.nsa.gov/about/mission-strategy/ (дата обращения 18.05.2017 г.).

[82] Central Security Service [Электронный ресурс] // National Security Agency: сайт. – URL: https://www.nsa.gov/about/central-security-service/ (дата обращения 17.05.2017 г.).

Деятельность АНБ неоднократно являлась предметом политических разногласий, таких как шпионаж за лидерами государств и экономический шпионаж. В 2013 году некоторые секретные программы наблюдения АНБ были показаны общественности Эдвардом Сноуденом.

Согласно предоставленным документам, АНБ перехватывает сообщения более миллиарда людей по всему миру, большинство которых являются гражданами Соединенных Штатов, и отслеживает движение сотен миллионов людей, пользующихся мобильными телефонами. На международном уровне исследования указывают на способность АНБ осуществлять надзор за внутренним интернет-трафиком зарубежных стран посредством «бумеранга маршрутизации». Бумеранг маршрутизации возможен, когда осуществляется передача любых данных через Интернет, которая возникает и завершается в одной стране, параллельно проходит через другую, в данном случае через США. Исследования, проведенные в Университете Торонто, показали, что примерно 25% внутреннего трафика Канады могут подвергаться перехвату АНБ в результате таких действий[83].

Секретная служба США (The U.S. Secret Service)[84] ведет деятельность по борьбе с электронными преступлениями, которые сосредоточены на выявлении и задержании международных киберпреступников, связанных с кибер-взломами, банковским мошенничеством, похищением данных и другими компьютерными преступлениями. Секция кибербезопасности Секретной службы непосредственно способствовала аресту транснациональных киберпреступников, виновных в хищении сотен миллионов номеров кредитных карт, и потере около 600 млн. долл. финансовых и торговых учреждений.

Секретная служба также руководит Национальным компьютерным судебным институтом, который проводит для сотрудников правоохранительных органов,

---

[83] Obar, Jonathan A.; Clement, Andrew (2013). «Internet Surveillance and Boomerang Routing: A Call for Canadian Network Sovereignty» [Электронный ресурс] // Proceedings of the Technology & Emerging Media Track – Annual Conference of the Canadian Communication Association. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2311792 (дата обращения 24.05.2017 г.).

[84] About the Secret Service [Электронный ресурс] // The U.S. Secret Service: сайт. – URL: https://www.secretservice.gov/ (дата обращения 06.05.2017 г.).

прокуроров и судей кибер-тренинги и предоставляет информацию для борьбы с киберпреступностью.

Таким образом можно сделать вывод, что система обеспечения информационной безопасности резко изменилась после событий 11 сентября 2001 года. Под предлогом борьбы с международным терроризмом осуществляется тотальной сбор и анализ информации из телекоммуникационных сетей, в том числе и личная информация самих граждан США находится под постоянным контролем. Но при погоне за эффективным обеспечением информационной безопасности государство пренебрегает правами человека на неприкосновенность частной жизни, о чем свидетельствует бывший сотрудник Агентства национальной безопасности США Э.Сноуден[85] в своих заявлениях.

Важно отметить, что основу информационной безопасности США составляет именно кибербезопасность. Осуществление кибербезопасности ведется не «пассивными» методами, а проводится активная деятельность по выявлению, предотвращению, ликвидации, а также проводятся контратаки на системы противника, с целью вывода из строя, либо завладения секретной информацией. Каждое военное ведомство имеет отдел либо службу по обеспечению кибербезопасности своих систем.

[85] Edward Snowden did enlist for special forces, US army confirms [Электронный ресурс] // The Guardian: сайт. – URL: https://www.theguardian.com/world/2013/jun/10/edward-snowden-army-special-forces (дата обращения 13.05.2017 г.).

ГЛАВА 2. ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ.

2.1 Характеристика угроз информационной безопасности Российской Федерации

Согласно ГОСТ Р 50922-2006[86] угрозой информационной безопасности является совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

В этом же документе содержится определения понятия «источник угрозы безопасности информации» – это субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

В действующей на данный момент Доктрине информационной безопасности Российской Федерации[87] основным угрожающим фактором, влияющим на информационную безопасность, является наращивание зарубежными странами возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях.

Параллельно ведется активная деятельность организаций и специальных служб, осуществляющих техническую разведку в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса, с целью завладения секретной и особо важной информацией.

Расширяются масштабы использования специальными службами определенных методов информационно-психологического воздействия, направленного на дестабилизацию социальной и внутриполитической ситуации в различных регионах мира и приводящих к подрыву суверенитета, нарушению

---

[86] Защита информации. Основные термины и определения: ГОСТ Р 50922-2006. – Введен 2008–02–01. – М.: Стандартинформ, 2008. С. 27.

[87] Собрание законодательства РФ. –2016. – N 50. – Ст. 7074.

территориальной целостности других государств. Для такой деятельности активно используются возможности информационных технологий, а также вовлекаются этнические и религиозные, правозащитные и иные организации.

В зарубежных СМИ увеличивается тенденция предоставления материалов, содержащих предвзятую оценку государственной политики Российской Федерации, а российские СМИ за рубежом зачастую подвергаются дискриминации, журналистам создают препятствия для выполнения их профессиональной деятельности.

Наращивается информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей.

Основную опасность мы видим от информационно-телекоммуникационной сети Интернет. В Интернете, при желании, можно найти информацию практически любого содержания, в том числе такую, которая может оказать пагубное влияние на подрастающее поколение. Также мы считаем, что угрозой являются и социальные сети, с помощью которых возможна как вербовка в запрещенные организации, так и склонение к причинению вреда себе или даже доведение до самоубийства[88].

В погоне за «популярностью» в социальных сетях подростки часто совершают необдуманные поступки, транслируя это в прямом эфире, либо выкладывая видео запись на страницы социальных сетей позже. К примеру трагедия, случившаяся осенью 2016 года в Пскове, когда двое 15 летних подростков сбежали от родителей, спрятались в загородном доме и обстреливали из ружья приехавшую полицейскую машину. Все свои действия они транслировали в прямом эфире на свои страницы в социальных сетях. В итоге все закончилось самоубийством[89].

Также при грамотном руководстве с помощью социальных сетей можно собирать вместе огромное количество население в определенном месте. Мероприятие может быть, как развлекательного характера, празднование или

---

[88] Козлов Д.Е. Влияние «вредной» информации на подростков // VIII Междунар. науч.–практич. конф. «Инновационные научные исследования: теория, методология, практика» // Наука и Просвещение, 2017. С. 207.

[89] Псковские Бонни и Клайд: смерть в Интернете [Электронный ресурс] // Вести.ru: сайт. – URL: http://www.vesti.ru/doc.html?id=2821576 (дата обращения 18.05.2017 г.).

митинг и т.д., так и мероприятия, которые могут вызвать негативные последствия и массовые беспорядки. Примером таких событий может служить беспорядки на болотной площади в Москве в мае 2012, возникшие в результате протестных акций. По разным оценкам на площади собралось от 8 до 30 тыс. человек[90]. Активная агитация проводилась через социальные сети.

Террористические организации для связи между собой и для осуществления своей деятельности пользуются теми же средствами связи, что и обычные граждане– социальными сетями и операторами мобильных сетей связи. Также активно используют технологии информационного воздействия на индивидуальное и общественное сознание с целью привлечения новых сторонников или вызвать социальную и межнациональную напряженность, разжигания религиозной ненависти и вражды, пропаганды экстремистской идеологии.

Неуклонно растет количество компьютерной преступности такой как распространение вредоносных программ, взлом и похищение информации ограниченного доступа, в том числе ПДн и личной переписки, так и похищение денежных средств с банковских карт, посредством осуществления переводов через Интернет на такие сервисы как, например, Яндекс Мани.

Регистрация в данной системе возможна без удостоверения личности. Чтобы создать счет на подобном ресурсе, необходим только выход в Интернет и любой активный номер телефона для получения смс. Счет является анонимным. Согласно тарифам[91] ресурса с анонимного счета можно осуществлять операции на сумму не более 15 тыс. рублей в сутки, но это является вполне крупной суммой и достаточной для совершения мошеннических действий.

Проблема еще состоит в том, что в силу совей наивности или невысокой грамотности в области информационной безопасности клиенты банков самостоятельно сообщают преступникам данные своих платежных карт, вплоть до

---

[90] Массовые акции в Москве 6 мая 2012 года [Электронный ресурс] // РИА Новости: сайт. – URL: https://ria.ru/trend/moscow_meetings_06052012/ (дата обращения 07.05.2017 г.).

[91] Лимиты: ограничения размеров операций [Электронный ресурс] // Яндекс.Денги: сайт. – URL: https://money.yandex.ru/page?id=523014 (дата обращения 26.05.2017 г.).

одноразового пароля от системы 3D-Secure[92], который поступает владельцу карты для подтверждения оплаты или перевода. В сообщении даже содержится указание «никому не сообщать пароль, даже сотрудникам банка», однако многие обманутые не обращают внимание на это предупреждение.

До сих пор остается довольно высокий уровень зависимости отечественной промышленности от зарубежных информационных технологий это касается программного обеспечения, электронных микросхем и плат, вычислительной техники и средств связи. А также низкий уровень внедрения отечественных разработок, недостаточность кадровым обеспечением в области информационной безопасности, низкой осведомленность граждан в вопросах обеспечения личной информационной безопасности.

В методике определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной ФСТЭК[93] в 2008 году под угрозами безопасности ПДн при их обработке в ИСПДн понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в ИСПДн.

Угрозы безопасности ПДн могут быть реализованы за счет утечки ПДн по техническим каналам (технические каналы утечки информации, обрабатываемой в технических средствах ИСПДн, технические каналы перехвата информации при ее передаче по каналам связи, технические каналы утечки акустической (речевой) информации) либо за счет несанкционированного доступа с использованием соответствующего программного обеспечения.

---

[92] Протокол 3D-Secure предназначен для безопасной оплаты картой товаров и услуг в Интернете. Клиенту посылается в смс одноразовый числовой пароль для подтверждения оплаты/перевода.

[93] Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных: утв. ФСТЭК РФ от 14.02.2008 г. [Электронный ресурс]. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=77814/ (дата обращения 07.05. 2017 г.).

При регистрации в социальных сетях пользователем вводятся практически полная информация о себе от ФИО и даты рождения, до места и сроков обучения, места работы и т.д. Также с помощью социальных сетей довольно просто найти необходимого человека, узнать круг его общения. По личным фото даже можно узнать марку автомобиля и гос.номер. Конечно же при условии, что этот человек пользуется социальной сетью и выкладывает свои личные фото, однако в большинстве случаев так и есть. Например, самая популярная социальная сеть на территории РФ «Вконтакте» насчитывает около 431 млн. пользователей[94], а согласно статистике SimilarWeb[95] 62.22% пользователей из РФ, 17.55% из Украины, 4.50% из Беларуси и 2.43% из Казахстана. Остальные 13.3 % распределились по странам Европы. Также в социальных сетях используется функция «геолокация», с помощью которой на сделанной фотографии отображаются название улицы или даже название заведения и указано расположение на карте.

Как показывает статистика Аналитического центра InfoWatch[96] за 2016 год зарегистрировано 1556 случаев утечки конфиденциальной информации. Это на 3,4% больше, чем в 2015 году. Виновниками утечек в 55.4% случаев стал внешний злоумышленник, однако на «втором» месте в 33.9% оказался действующий сотрудник. Остальные 10.7% остались за подрядчиком, руководителем, бывшим сотрудником и системным администратором.

Среди раскрытой информации к персональным данным относится 85.6%, к платежной информации относится 7.3%, к государственной тайне 1.7%, к коммерческой 5.4%.

За 2016 год в мире было скомпрометировано более 3,147 млрд. записей персональных данных– это в три раза больше, чем за 2015 год.

---

[94] Каталог пользователей ВКонтакте [Электронный ресурс] // сайт ВКонтакте: сайт. – URL: https://vk.com/catalog.php?selection=430-98 (дата обращения 03.05.2017 г.).

[95] Traffic Overview vk.com [Электронный ресурс] // SimilarWeb: сайт. – URL: https://www.similarweb.com/website/vk.com#overview (дата обращения 03.05.2017 г.).

[96] Глобальное исследование утечек конфиденциальной информации в 2016 году [Электронный ресурс] // Группа Компаний InfoWatch: сайт. – URL: https://www.infowatch.ru/report2016 (дата обращения 10.05.2017 г.).

Согласно Стандарту Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»[97] к основными источниками угроз информационной безопасности относятся:

- неблагоприятные события природного, техногенного и социального характера;
- террористы и криминальные элементы;
- зависимость от поставщиков/провайдеров/партнеров/клиентов;
- сбои, отказы, разрушения/повреждения программных и технических средств;
- работники организации банковской системы РФ, реализующие угрозы информационной безопасности с использованием легально предоставленных им прав и полномочий (внутренние нарушители информационной безопасности);
- работники организации банковской системы РФ, реализующие угрозы информационной безопасности вне легально предоставленных им прав и полномочий, а также субъекты, не являющиеся работниками организации банковской системы РФ, но осуществляющие попытки несанкционированного доступа (внешние нарушители информационной безопасности);
- несоответствие требованиям надзорных и регулирующих органов, действующему законодательству.

Наиболее актуальные источники угроз на физическом уровне, уровне сетевого оборудования и уровне сетевых приложений:

- внешние нарушители ИБ: лица, разрабатывающие/распространяющие вирусы и другие вредоносные программные коды; лица, организующие DoS, DDoS и иные виды атак; лица, осуществляющие попытки НСД и НРД;
- внутренние нарушители информационной безопасности: персонал, имеющий права доступа к аппаратному оборудованию, в том числе сетевому, администраторы серверов, сетевых приложений и т.п.;
- комбинированные источники угроз: внешние и внутренние нарушители информационной безопасности, действующие совместно и (или) согласованно;

---

[97] Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения СТО БР ИББС-1.0-2014: Стандарт Банка России от 17.05.2014 г. N Р-399: по сост. на 23 мая 2017 г. // Вестник Банка России. – N 48-49. – 2014.

- сбои, отказы, разрушения/повреждения программных и технических средств.

Наиболее актуальные источники угроз на уровнях операционных систем, систем управления базами данных, банковских технологических процессов:

-внутренние нарушители информационной безопасности: администраторы ОС, пользователи банковских приложений и технологий, администраторы информационной безопасности и т.д.;

- комбинированные источники угроз: внешние и внутренние нарушители информационной безопасности, действующие в сговоре

На данных уровнях и уровне бизнес-процессов реализация угроз внешними нарушителями информационной безопасности, действующими самостоятельно без соучастия внутренних, практически невозможна.

Наиболее актуальные источники угроз на уровне бизнес-процессов:

- внутренние нарушители информационной безопасности: авторизованные пользователи и операторы АБС, представители менеджмента организации и пр.;

- комбинированные источники угроз: внешние нарушители информационной безопасности (например, конкуренты) и внутренние, действующие в сговоре;

- несоответствие требованиям надзорных и регулирующих органов, действующему законодательству.

Интересную статистику приводит «Лаборатория Касперского» в своем отчете «Развитие информационных угроз в первом квартале 2017 года»[98]. Согласно отчету за первый квартал 2017 года было зафиксировано более 479.53 млн. атак на компьютеры и мобильные устройства пользователей, при этом атаки проводились из 190 стран мира.

Пресечено 288 тыс. попыток кражи денежных средств через Интернет с банковских карт клиентов, с использованием вредоносного программного обеспечения.

---

[98] Развитие информационных угроз в первом квартале 2017 года. Статистика [Электронный ресурс] // АО «Лаборатория Касперского»: сайт. – URL: https://securelist.ru/analysis/malware-quarterly/30657/it-threat-evolution-q1-2017-statistics/ (дата обращения 16.05.2017 г.).

Всего зафиксировано более 174.99 млн. новых вредоносных и потенциально опасных объектов.

Таким образом можно сделать вывод, что в связи с событиями последних годов таких как вхождение Крыма в состав РФ и успешные боевые действия в Сирии, в отношении нашей страны у специальных и разведывательных служб зарубежных стран возник новый интерес.

Можно с уверенностью сказать, что практически все угрозы информационной безопасности поступают из информационно-телекоммуникационных сетей, в том числе и Интернет. Будь то угрозы для подростков в виде «вредной информации» или мошенничество и кражи средств с банковских карт.

Также из статистики, приведенной выше, можно сделать вывод, что ценность персональных данных и интерес к ним за последний год возрос в три раза, либо защите такой информации уделяется не достаточно должное внимание во всем мире.

2.2 Меры по обеспечению информационной безопасности Российской Федерации.

Доктрина информационной безопасности Российской Федерации[99] 2016 года закрепляет, что обеспечение информационной безопасности осуществляется с помощью взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления.

В Доктрине информационной безопасности Российской Федерации[100] 2000 года во втором разделе были установлены методы обеспечения информационной безопасности Российской Федерации. К таким методам относились правовые,

---

[99] Собрание законодательства РФ. 12.12.2016. – N 50. – Ст. 7074.
[100] Российская газета. – N 187. –2000.

организационно - технические и экономические, а также подробно раскрывалась суть каждого из них.

Статья 16 Федерального закона № 149-ФЗ[101] содержит, что защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

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

–соблюдение конфиденциальности информации ограниченного доступа;

–реализацию права на доступ к информации.

Из всего перечня информации с ограниченным доступом конкретизирующие требования к защите такой информации установлены в отношении следующих видов сведений:

-Государственная тайна. Основные положения защиты сведений составляющих государственную тайну закреплены в пятом разделе Закона РФ N 5485-1 «О государственной тайне»[102].

Согласно Постановлению Правительства РФ N 608 «О сертификации средств защиты информации»[103] обязательной сертификации подлежат средства (технические, криптографические, программные и другие), с помощью которых обеспечивается защита сведений, отнесенный к государственной тайне. Систему сертификации создают ФСТЭК, ФСБ и МО РФ.

В соответствии с Указом Президента РФ № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»[104] определяются условия, при которых возможно подключение к

---

[101] Собрание законодательства РФ. – 2006 г. – N 31 (1 ч.). – Ст. 3448.

[102] Собрание законодательства РФ. – 1997 г. – N 41. – Стр. 8220-823.

[103] О сертификации средств защиты информации: постановление Правительства РФ от 26.06.1995 г. N 608: по сост. на 10 мая 2017 г. // Собрание законодательства РФ. – 1995. – N 27. – Ст. 2579.

[104] О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена: указ Президента РФ от 17.03.2008 г. N 351: по сост. на 16 мая 2017 г. // Собрание законодательства РФ. – 2008. – N 12. – Ст. 1110.

информационно-телекоммуникационным сетям для обмена информацией, составляющей государственную тайну.

-Государственные информационные системы. К государственным информационным системам предъявляются особые требования к защите информации, содержащейся в них.

Такие требования закреплены во многих подзаконных актах. Среди прочих важно отметить Приказ ФСТЭК N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»[105]. К таким требованиям относятся: аутентификация и идентификация субъектов и объектов доступа; управление доступом субъектов доступа к объектам доступа; ограничение программной среды; защита машинных носителей информации; регистрация событий безопасности; антивирусная защита; обнаружение/предотвращение вторжений; контроль защищенности информации; целостность информационной системы и информации; доступность информации; защита среды виртуализации; защита информационной системы, ее средств, систем связи и передачи данных.

Кроме описанного выше Приказа положения защиты информации в государственных информационных системах установлены в следующих актах:

Президента РФ № 351 «О мерах по обеспечению информационной безопасности российской федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

Постановление Правительства РФ № 424 «Об особенностях подключения федеральных государственных систем к информационно-телекоммуникационным сетям»[106], в соответствии с которым операторы государственных информационной системы обязаны обеспечить защиту информации, содержащейся в информационных системах общего пользования, от уничтожения, изменения и

[105] Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России от 11.02.2013 г. N 17: по сост. на 16 мая 2017 г. // Российская газета. – N 136. – 2013.

[106] Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям: постановление Правительства РФ от 18.05.2009 г. N 424: по сост. на 29 апреля 2017 г. // Собрание законодательства РФ. – 2009. – N 21. – Ст. 2573.

блокирования доступа к ней. Осуществлять постоянный контроль возможности доступа неограниченного круга лиц к информационным системам общего пользования. Восстановить, измененную или уничтоженную вследствие НСД информацию, в срок до 8 часов;

Приказ Минкомсвязи N 149 «Об утверждении Требований к технологическим, программным и лингвистическим средствам, необходимым для размещения информации государственными органами и органами местного самоуправления в сети Интернет в форме открытых данных, а также для обеспечения ее использования»[107].

В пункте 6 Приказа Минкомсвязи N 149 указано, что государственными органами и органами местного самоуправления устанавливаются требования к средствам защиты информации, с помощью которых обеспечивается доступ к общедоступной информации, определяющиеся с учетом положений:

1) Приказа Минкомсвязи N 104 «Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования»[108]. Согласно этому Приказу безопасность информационной системы общего пользования – это её способность противостоять попыткам несанкционированного доступа к техническим и программным средствам системы и преднамеренным дестабилизирующим внутренним или внешним информационным воздействиям, следствием которых может быть нарушение ее функционирования.

2) Приказа ФСБ и ФСТЭК N 416/N 489 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего

---

[107] Об утверждении Требований к технологическим, программным и лингвистическим средствам, необходимым для размещения информации государственными органами и органами местного самоуправления в сети «Интернет» в форме открытых данных, а также для обеспечения ее использования: приказ Минкомсвязи России от 27.06.2013 г. N 149: по сост. на 28 апреля 2017 г. // Российская газета. – N 187. – 2013.

[108] Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования: приказ Минкомсвязи РФ от 25.08.2009 N 104: по сост. на 15 мая 2017 г. // Российская газета. – N 188. – 2009.

пользования»[109]. Пункт 12 содержит мероприятия по обеспечению информационной безопасности. К ним относятся:

–определение и моделирование угроз,

–разработка в соответствии с моделью угроз систем защиты информации;

–тестирование перед использованием средств защиты информации и составление заключения о возможности их эксплуатации;

–установка и ввод в эксплуатацию средств защиты в соответствии с документацией (эксплуатационной, технической);

–обучение персонала, использующих средства защиты информации при работе в системе общего пользования, правилам работы с ними;

–учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

–контроль за использованием средств защиты информации, предусмотренный эксплуатационной и технической документацией;

–проведение разбирательств по фактам несоблюдения условий использования средств защиты информации, которые могут привести к нарушению безопасности информационной системы или другим нарушениям, а также разработка мер по предотвращению возможных последствий подобных нарушений.

Приказ ФСО N 443 «Об утверждении Положения о российском государственном сегменте информационно-телекоммуникационной сети «Интернет»[110]. В Приказе установлено, что Служба специальной связи и информации Федеральной службы охраны Российской Федерации организует поддержание, обеспечивает эксплуатацию, развитие и информационную безопасность сети, в том числе с использованием ведомственного сегмента государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

---

[109] Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования: приказ ФСБ РФ N 416, ФСТЭК РФ N 489 от 31.08.2010 г.: по сост. на 15 мая 2017 г. // Российская газета. – N 240. – 2010.

[110] Об утверждении Положения о российском государственном сегменте информационно-телекоммуникационной сети «Интернет»: приказ ФСО России от 07.09.2016 г. N 443: по сост. на 12 мая 2017 г. // Российская газета. – N 242. – 2016.

Приказ Минэкономразвития N 470 «О Требованиях к технологическим, программным и лингвистическим средствам обеспечения пользования официальными сайтами федеральных органов исполнительной власти»[111]. Требования к средствам защиты информации официальных сайтов должны соответствовать пунктам 2 и 3 Постановления Правительства Российской Федерации N 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям».

С целью защиты информации, размещенной на официальном сайте, должно быть обеспечено:

–применение электронной подписи или иных аналогов собственноручной подписи при размещении, изменении или удалении информации на официальном сайте;

–ведение электронных журналов учета операций, выполненных с помощью программного обеспечения и технологических средств ведения официального сайта, содержащих учет всех действий по размещению, изменению и удалению информации на официальном сайте, время этих действий, содержание изменений и информацию о сотруднике или операторе официального сайта, осуществившем действия на сайте;

–ежедневное копирование всей размещенной на официальном сайте информации и электронных журналов учета на резервный материальный носитель, с возможностью восстановления;

–защита информации от уничтожения, искажения, блокировки доступа к ней и иных неправомерных действий;

–применение шифрованных транспортных механизмов и сертификатов безопасности при передаче данных, обеспечивающих шифрование и защиту передаваемой информации, в том числе персональных данных пользователей официальных сайтов.

---

[111] О Требованиях к технологическим, программным и лингвистическим средствам обеспечения пользования официальными сайтами федеральных органов исполнительной власти: приказ Минэкономразвития России от 16.11.2009 г. N 470: по сост. на 12 мая 2017 г. // Российская газета. – N 15. – 2010.

Также важно отметить, что согласно ч. 2.1 статьи 13 Федерального закона № 149-ФЗ технические средства информационных систем, используемые государственными органами, органами местного самоуправления, государственными и муниципальными унитарными предприятиями или государственными и муниципальными учреждениями, размещаются на территории РФ.

-Банковская тайна. Центральный банк России является основной организацией, регулирующей банковскую сферу в обеспечении информационной безопасности. Регулирование и обеспечение информационной безопасности банковской сферы включает следующие документы:

Положение Банка России N 397-П «О порядке создания, ведения и хранения баз данных на электронных носителях»[112] обязует кредитные организации самостоятельно определять способы и средства обеспечения информационной безопасности при создании, ведении и хранении таких баз данных, а также исключить возможность порчи, несанкционированного изменения или доступа, заражения вредоносными программами, утраты информации в базах данных.

Положение Банка России N 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»[113]. В соответствии с Положением Банк России проводит контроль за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств, в виде проверок операторов платежных систем, в том числе и инспекционных проверок, а также запрашивает и получает у операторов платежных систем необходимые документы и информацию о выполнение требований обеспечения защиты информации при переводах денежных средств.

---

[112] Положение о порядке создания, ведения и хранения баз данных на электронных носителях: утв. Банком России о 21.02.2013 г. N 397-П: по сост. на 23 мая 2017 г. // Вестник Банка России. – N 23. – 2013.

[113] Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств: утв. Банком России от 09.06.2012 г. N 382-П: по сост. на 23 мая 2017 г. // Вестник Банка России. – N 32. – 2012.

Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения»[114] был разработан с целью проверки уровня ИБ Центрального Банка России, а также всех организаций банковской системы Российской Федерации.

Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014»[115] Настоящий стандарт устанавливает способы определения степени выполнения требований стандарта Банка России СТО БР ИББС-1.0-2014, указанного выше.

Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности»[116], направленны на реализацию организациями банковской системы обнаружений и устранения инцидентов информационной безопасности.

Письмо Банка России «О рекомендациях по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности»[117]. Рекомендации были подготовлены с целью противодействия распространения вредоносных программ, способным нанести ущерб программному обеспечению, системам и оборудованию кредитных организаций. Вследствие чего также

---

[114] Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014 «СТО БР ИББС-1.2-2014»: Стандарт Банка России от 17.05.2014 г. N Р-399: по сост. на 23 мая 2017 г. // Вестник Банка России. – N 48-49. – 2014.

[115] Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014 «СТО БР ИББС-1.2-2014»: Стандарт Банка России от 17.05.2014 г. N Р-399: по сост. на 27 мая 2017 г. // Вестник Банка России. – N 48-49. – 2014.

[116] Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности» РС БР ИББС-2.5-2014: введены в действие Распоряжением Банка России от 17.05.2014 г. N Р-400: по сост. на 27 мая 2017 г. // Вестник Банка России. – N 48-49. – 2014.

[117] О рекомендациях по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности: письмо Банка России от 24.03.2014 г. N 49-Т: по сост. на 27 мая 2017 г. // Вестник Банка России. – N 34. – 2014.

возможна утрата, изменение и утечка конфиденциальной информации о деятельности кредитной организации, а также персональных данных.

-Персональные данные. Федеральный закон N 152-ФЗ «О персональных данных»[118] в статье 19 закрепляет основные положения о необходимых мерах по безопасности ПДн при их обработке. В частности, также указано, что оператор обязан обеспечивать защиту ПДн, путем принятия необходимых правовых, организационных и технических мер от несанкционированного доступа к ПДн, уничтожения, блокирования, изменения, копирования, утечки и иных неправомерных действий.

Дополняют данную статью, принятые Правительством РФ постановления:

Постановление Правительства N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Защита ПДн включает в себя организационные и технические меры, определенные в соответствии с актуальными угрозами безопасности ПДн. Оператор самостоятельно выбирает средства защиты информации для систем защиты ПДн в соответствии с нормативными правовыми актами, принятыми ФСТЭК и ФСБ. Контролирует выполнение требований оператор самостоятельно или с помощью юридических лиц, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

Постановление Правительства РФ N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»[119]

Оператор, который обрабатывает ПДн должен обеспечить раздельное хранение ПДн или материальных носителей, которые обрабатываются в различных целях. Обработка ПДн, должна осуществляться таким образом, чтобы можно было определить лиц, осуществивших обработку ПДн, а также установить места хранения

---

[118] Собрание законодательства РФ. – 2006. – N 31 (1 ч.). – Ст. 3451.

[119] Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации: постановление Правительства РФ от 15.09.2008 г. N 687: по сост. на 28 мая 2017 г. // Собрание законодательства РФ. – 2008. – N 38. – Ст. 4320.

ПДн или материальных носителей. При хранении материальных носителей должны соблюдаться условия сохранности ПДн исключающие неправомерный доступ.

Постановление Правительства РФ N 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»[120]

При обработке и хранении ПДн на материальных носителях оператор, обеспечивающий обработку данных должен применять средства электронной подписи для обеспечения сохранности целостности и неизменности данных, занесенных на материальный носитель. Также, в соответствии с законодательством Российской Федерации используются криптографические средства защиты данных.

В Приказе ФСТЭК N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» конкретизируются организационные и технические меры по защите ПДн.

К ним относятся:

–идентификация и аутентификация субъектов и объектов доступа;

–управление доступом;

–ограничение программной среды;

–защита машинных носителей информации, на которых хранятся или обрабатываются ПДн;

–регистрация событий безопасности;

–антивирусная защита;

–обнаружение (предотвращение) вторжений;

–анализ защищенности ПДн;

–обеспечение целостности информационной системы и ПДн;

–обеспечение доступности ПДн;

–защита среды виртуализации;

---

[120] Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных: постановление Правительства РФ от 06.07.2008 г. N 512: по сост. на 25 мая 2017 г. // Собрание законодательства РФ. – 2008. – N 28. – Ст. 3384.

–защита технических средств;

–защита информационной системы, ее средств, систем связи и передачи данных;

–выявление инцидентов, которые могут привести к сбоям или нарушению функционирования информационной системы или к возникновению угроз безопасности ПДн, и реагирование на них;

–управление конфигурацией информационной системы и системы защиты ПДн.

За нарушение требований законодательства в сфере информационной безопасности установлена дисциплинарная, гражданско-правовая, административная и уголовная ответственность.

За нарушение законодательства Российской Федерации о государственной тайне предусмотрена следующая ответственность:

Уголовная в соответствии с УК РФ[121]:

Ст. 275 Государственная измена;

Ст. 276 Шпионаж;

Ст. 283 Разглашение государственной тайны;

Ст. 284 Утрата документов, содержащих государственную тайну.

Административная в соответствии с КоАП:

Ст. 13.12. Нарушение правил защиты информации;

Ст. 13.12. Нарушение правил защиты информации;

Ст. 13.13. Незаконная деятельность в области защиты информации;

Ст. 13.14. Разглашение информации с ограниченным доступом;

Ст. 14.49. Нарушение обязательных требований в отношении оборонной продукции.

Также предусмотрена гражданско-правовая или дисциплинарная ответственность в соответствии с действующим законодательством.

---

[121] Уголовный кодекс Российской Федерации от 13.06.1996 г. N 63-ФЗ: по сост. на 28 мая 2017 г. // Собрание законодательства РФ. –1996. – N 25. – Ст. 2954.

За правонарушения в сфере информации, информационных технологий и защиты информации предусмотрена административная ответственность в соответствии с КоАП[122]:

Ст. 13.12. Нарушение правил защиты информации;

Ст. 13.13. Незаконная деятельность в области защиты информации;

Также нарушение требований Федерального закона №149-ФЗ влечет за собой дисциплинарную, гражданско-правовую, или уголовную ответственность в соответствии с законодательством РФ.

Ответственность за нарушение Федерального закона N 98-ФЗ «О коммерческой тайне» установлена следующая:

Гражданско-правовая в соответствии с ГК РФ:

Ст. 1472. Ответственность за нарушение исключительного права на секрет производства[123];

Ст. 15. Возмещение убытков[124].

Административная в соответствии с КоАП ст. 13.14. Разглашение информации с ограниченным доступом.

Уголовная в соответствии с УК РФ[125] ст. 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.

Также в соответствии с законодательством предусмотрена дисциплинарная ответственность.

За нарушение требований Федерального закона N 152-ФЗ «О персональных данных» предусмотрена следующая ответственность:

Административная в соответствии с КоАП[126]:

---

[122] Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ по сост. на 28 мая 2017 г. // Собрание законодательства РФ. – 2002. – N 1 (ч. 1). – Ст. 1.

[123] Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ по сост. на 28 мая 2017 г. // Собрание законодательства РФ. – 2006. N 52 (1 ч.). – Ст. 5496.

[124] Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 г. N 51-ФЗ: по сост. на 28 мая 2017 г. // Собрание законодательства РФ. –1994. – N 32. – Ст. 3301.

[125] Собрание законодательства РФ. –1996. – N 25. – Ст. 2954.

[126] Собрание законодательства РФ. – 2002. – N 1 (ч. 1). – Ст. 1.

Ст. 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных);

Ст. 13.12. Нарушение правил защиты информации;

Ст. 13.13. Незаконная деятельность в области защиты информации;

Ст. 13.14. Разглашение информации с ограниченным доступом.

Уголовная в соответствии с УК РФ:

Ст. 137. Нарушение неприкосновенности частной жизни;

Ст. 272. Неправомерный доступ к компьютерной информации.

Также предусмотрена дисциплинарная ответственность в соответствии с законодательством.

За разглашение банковской тайны предусмотрена следующая ответственность:

Гражданско-правовая в соответствии с ГК РФ ст. 857. Банковская тайна[127];

Административная в соответствии с КоАП ст. 13.14. Разглашение информации с ограниченным доступом;

Уголовная в соответствии с УК РФ ст. 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.

Подводя итог можно сделать вывод, что к мерам обеспечения информационной безопасности относятся такие как правовые, организационные и технические.

Государственные органы всеми возможными законными способами стараются обеспечить информационную безопасность страны, общества и личности.

Важно также обратить внимание на угрозы исходящие от информационно-телекоммуникационных сетей. Например, события конца 2016 начала 2017 года, в результате которых подростков через социальные сети склоняли к причинению себе вреда и даже к совершению самоубийства[128].

---

[127] Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 г. N 14-ФЗ: по сост. на 24 мая 2017 г. // Собрание законодательства РФ. –1996. – N 5. – Ст. 410.

[128] Козлов Д.Е. Влияние «вредной» информации на подростков // VIII Междунар. науч.–практич. конф. «Инновационные научные исследования: теория, методология, практика» // Наука и Просвещение, 2017. С. 207.

На данный момент реализован механизм с блокировкой и ограничение доступа к подобным материалам, посредством добавления в Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено. Проведением данных работ и постоянным мониторингом информационных сетей занимается Роскомнадзор. Но мы видим эти меры не достаточными и считаем также необходимым привлекать к административной ответственности создателей, администраторов, модераторов и всех причастных к подобным деяниям лиц.

В настоящее время Уголовный кодекс не содержит нормы за склонение совершения суицида через «Интернет». В связи с этим целесообразно в кротчайшие сроки ввести ответственность за совершение подобных деяний. Ведь подростки, в силу своего возраста могут поддаваться на манипулирование и уловки заинтересованных лиц.

Также, как мы считаем, необходимо создание и введение специальных курсов или проведение образовательных бесед на «классных часах» по информационной безопасности (безопасности персональных данных, а также ограждение детей от вредной информации) с начальных классов образовательных учреждений с целью повышением грамотности населения, а также информационные ролики подобной направленности, транслируемые по федеральным каналам СМИ и в популярных социальных сетях (vk.com, youtube.com, rutube.ru, facebook.com и т.п.).

ЗАКЛЮЧЕНИЕ

Подводя итог, проведенного исследования необходимо отметить, что в новой Доктрине информационной безопасности Российской Федерации законодатель попытался дать точное определение информационной безопасности «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства», однако данное определение совпадает с определением «национальная безопасность Российской Федерации», закрепленным в Стратегии национальной безопасности Российской Федерации от 31 декабря 2015 года «состояние защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан Российской Федерации, достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации» добавилось слово «информационных».

Субъектами, обеспечивающими информационную безопасность личности, общества и государства в Российской Федерации являются:

Президент Российской Федерации;

Совет Федерации и Государственная Дума (Комитет Государственной Думы по безопасности и противодействию коррупции);

Правительство Российской Федерации;

Совет безопасности Российской Федерации (Межведомственная комиссия Совета Безопасности Российской Федерации);

Министерство обороны Российской Федерации (Восьмое управление Генерального штаба Вооруженных Сил Российской Федерации);

Служба внешней разведки Российской Федерации;

Федеральная служба безопасности Российской Федерации;

Федеральная служба охраны Российской Федерации;

Федеральная служба по техническому и экспортному контролю;

Государственная фельдъегерская служба Российской Федерации;

Центральный Банк России;

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций;

Министерство внутренних дел Российской Федерации (Департамент информационных технологий, связи и защиты информации Министерства внутренних дел Российской Федерации. Управление «К» МВД России).

Система обеспечения информационной безопасности США резко изменилась после событий 11 сентября 2001 года. Под предлогом борьбы с международным терроризмом осуществляется тотальной сбор и анализ информации из телекоммуникационных сетей, в том числе и личная информация самих граждан США находится под постоянным контролем. Но при погоне за эффективным обеспечением информационной безопасности государство пренебрегает правами человека на неприкосновенность частной жизни, о чем свидетельствует бывший сотрудник Агентства национальной безопасности США Э.Сноуден в своих заявлениях.

Важно отметить, что основу информационной безопасности США составляет именно кибербезопасность. Осуществление кибербезопасности ведется не «пассивными» методами, а проводится активная деятельность по выявлению, предотвращению, ликвидации, а также проводятся контратаки на системы противника, с целью вывода из строя, либо завладения секретной информацией. Каждое военное ведомство имеет отдел либо службу по обеспечению кибербезопасности своих систем.

В связи с событиями последних годов таких как вхождение Крыма в состав Российской Федерации и успешные боевые действия наших вооруженных сил в Сирии, в отношении нашей страны у специальных и разведывательных служб зарубежных стран возник новый интерес.

Можно с уверенностью сказать, что практически все угрозы информационной безопасности поступают из информационно-телекоммуникационных сетей, в том числе и «Интернет». Будь то угрозы для подростков в виде «вредной информации» или мошенничество и кражи средств с банковских карт.

Из статистических данных можно сделать вывод, что, либо ценность персональных данных и интерес к ним за последний год возрос в три раза, либо защите такой информации уделяется не достаточно должное внимание во всем мире.

К мерам обеспечения информационной безопасности относятся такие как правовые, организационные и технические.

Государственные органы всеми возможными законными способами стараются обеспечить информационную безопасность страны, общества и личности.

Важно также обратить внимание на угрозы исходящие от информационно-телекоммуникационных сетей. Например, события конца 2016 начала 2017 года, в результате которых подростков через социальные сети склоняли к причинению себе вреда и даже к совершению самоубийства[129].

На данный момент реализован механизм с блокировкой и ограничение доступа к подобным материалам, посредством добавления в Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено. Проведением данных работ и постоянным мониторингом информационных сетей занимается Роскомнадзор.

Однако в настоящее время Уголовный кодекс не содержит нормы за склонение совершения суицида через «Интернет». В связи с этим целесообразно в кротчайшие сроки ввести ответственность за совершение подобных деяний. Ведь подростки, в силу своего возраста могут поддаваться на манипулирование и уловки заинтересованных лиц.

---

[129] Козлов Д.Е. Влияние «вредной» информации на подростков // VIII Междунар. науч.–практич. конф. «Инновационные научные исследования: теория, методология, практика» // Наука и Просвещение, 2017. С. 207.

Также, как мы считаем, необходимо создание и введение специальных курсов или проведение образовательных бесед на «классных часах» по информационной безопасности (безопасности персональных данных, а также ограждение детей от вредной информации) с начальных классов образовательных учреждений с целью повышением грамотности населения, а также информационные ролики подобной направленности, транслируемые по федеральным каналам СМИ и в популярных социальных сетях (vk.com, youtube.com, rutube.ru, facebook.com и т.п.).

СПИСОК ИСТОЧНИКОВ

1. Нормативные источники

1.1. Конституция Российской Федерации принята всенародным голосованием 12 декабря 1993 г.: по сост. на 27 марта 2017 г. // Собрание законодательства РФ. – 2014. – N 31. – Ст. 4398.

1.2. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 г. N 51-ФЗ: по сост. на 24 мая 2017 г. // Собрание законодательства РФ. –1994. – N 32. – Ст. 3301.

1.3. Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 г. N 14-ФЗ: по сост. на 24 мая 2017 г. // Собрание законодательства РФ. –1996. – N 5. – Ст. 410.

1.4. Уголовный кодекс Российской Федерации от 13.06.1996 г. N 63-ФЗ: по сост. на 24 мая 2017 г. // Собрание законодательства РФ. –1996. – N 25. – Ст. 2954.

1.5. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ по сост. на 24 мая 2017 г. // Собрание законодательства РФ. – 2002. – N 1 (ч. 1). – Ст. 1.

1.6. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ по сост. на 24 мая 2017 г. // Собрание законодательства РФ. – 2006. N 52 (1 ч.). – Ст. 5496.

1.7. О государственной тайне: закон от 21.07.1993 г. N 5485-1: по сост. на 03 апреля 2017 г. // Собрание законодательства РФ. – 1997 г. – N 41. – Стр. 8220-823.

1.8. О банках и банковской деятельности: федеральный закон от 02.12.1990 г. N 395-1: по сост. на 16 апреля 2017 г. // Собрание законодательства РФ. –1996. – N 6. – ст. 492.

1.9. О Федеральной службе безопасности: федеральный закон от 03.04.1995 г. N 40-ФЗ: по сост. на 29 марта 2017 г. // Собрание законодательства РФ. – 1995. – N 15. – Ст. 1269.

1.10. О внешней разведке: федеральный закон от 10.01.1996 г. N 5-ФЗ: по сост. на 01 апреля 2017 г. // Собрание законодательства РФ. – 1996. – N 3. – Ст. 143.

1.11. О государственной охране: федеральный закон от 27.05.1996 г. N 57-ФЗ: по сост. на 08 апреля 2017 г. // Собрание законодательства РФ. – 1996. – N 22. – Ст. 2594.

1.12. О коммерческой тайне: федеральный закон от 29.07.2004 г. N 98-ФЗ: по сост. на 03 мая 2017 г. // Собрание законодательства РФ. – 2004. – N 32. – Ст. 3283.

1.13. О персональных данных: федеральный закон от 27.07.2006 г. N 152-ФЗ: по сост. на 26 апреля 2017 г. // Собрание законодательства РФ. – 2006. – N 31 (1 ч.). – Ст. 3451.

1.14. Об информации, информационных технологиях и о защите информации: федеральный закон от 27.07.2006 г. N 149-ФЗ: по сост. на 28 апреля 2017 г. // Собрание законодательства РФ. – 2006 г. – N 31 (1 ч.). – Ст. 3448.

1.15. О безопасности: федеральный закон от 28.12.2010 г. N 390-ФЗ: по сост. на 25 апреля 2017 г. // Собрание законодательства РФ. – 2011. – N 1. – Ст. 2.

1.16. О защите детей от информации, причиняющей вред их здоровью и развитию: федеральный закон от 29.12.2010 N 436-ФЗ: по сост. на 16 мая 2017 г. // Собрание законодательства РФ. – 2011. – N 1. – Ст. 48.

1.17. Об инвестиционном товариществе: федеральный закон от 28.11.2011 г. N 335-ФЗ: по сост. на 18мая 2017 г. // Собрание законодательства РФ. – 2011. – N 49 (ч. 1). – Ст. 7013.

1.18. Об утверждении Перечня сведений, отнесенных к государственной тайне: указ Президента РФ от 30.11.1995 г. N 1203: по сост. на 26 марта 2017 г. // Собрание законодательства РФ. – 1995. – N 49. – Ст. 4775.

1.19. Доктрина информационной безопасности Российской Федерации: утв. Президентом РФ от 09.09.2000 г. N Пр-1895 // Российская газета. – N 187. –2000. (Документ утратил силу с 5 декабря 2016 года в связи с изданием Указа Президента РФ от 05.12.2016 N 646.)

1.20. Вопросы Федеральной службы безопасности Российской Федерации: указ Президента РФ от 11.08.2003 г. N 960: по сост. на 13 апреля 2017 г. // Собрание законодательства РФ. – 2003. – N 33. – Ст. 3254.

1.21. Вопросы Федеральной службы охраны Российской Федерации: указ Президента РФ от 07.08.2004 г. N 1013: по сост. на 23 марта 2017 г. // Собрание законодательства РФ. – 2004. – N 32. – Ст. 3314.

1.22. Вопросы Министерства обороны Российской Федерации: указ Президента РФ от 16.08.2004 г. N 1082: по сост. на 27 марта 2017 // Собрание законодательства РФ. – 2004. – N 34. – Ст. 3538.

1.23. Вопросы Федеральной службы по техническому и экспортному контролю: указ Президента РФ от 16.08.2004 г. N 1085: по сост. на 23 апреля 2017 г. // Собрание законодательства РФ. – 2004. – N 34. – Ст. 3541.

1.24. О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена: указ Президента РФ от 17.03.2008 г. N 351: по сост. на 16 мая 2017 г. // Собрание законодательства РФ. – 2008. – N 12. – Ст. 1110.

1.25. Положение о Совете Безопасности Российской Федерации: указ Президента РФ от 06.05.2011 г. N 590: по сост. на 30 марта 2017 г. // Собрание законодательства РФ. – 2011. – N 19. – Ст. 2721.

1.26. Положение о Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности: указ Президента РФ от 06.05.2011 г. N 590: по сост. на 03 апреля 2017 г. // Собрание законодательства РФ. – 2011. – N 19. – Ст. 2721.

1.27. Вопросы Государственной фельдъегерской службы Российской Федерации: указ Президента РФ от 07.04.2014 г. N 213: по сост. на 14 апреля 2017 г. // Собрание законодательства РФ. – 2014. – N 15. – Ст. 1726.

1.28. О Стратегии национальной безопасности Российской Федерации: указ Президента РФ от 31.12.2015 г. N 683: по сост. на 12 апреля 2017 г. // Собрание законодательства РФ. – 2016. – N 1 (часть II). – Ст. 212.

1.29. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 05.12.2016 г. N 646: по сост. на 30 марта 2017 г. // Собрание законодательства РФ. –2016. – N 50. – Ст. 7074.

1.30. О сертификации средств защиты информации: постановление Правительства РФ от 26.06.1995 г. N 608: по сост. на 10 мая 2017 г. // Собрание законодательства РФ. – 1995. – N 27. – Ст. 2579.

1.31. Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности: постановление Правительства РФ от 04.09.1995 г. N 870: по сост. на 30 апреля 2017 г. // Собрание законодательства РФ. – 1995. – N 37. – Ст. 3619.

1.32. Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных: постановление Правительства РФ от 06.07.2008 г. N 512: по сост. на 25 мая 2017 г. // Собрание законодательства РФ. – 2008. – N 28. – Ст. 3384.

1.33. Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации: постановление Правительства РФ от 15.09.2008 г. N 687: по сост. на 17 мая 2017 г. // Собрание законодательства РФ. – 2008. – N 38. – Ст. 4320.

1.34. О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций: постановление Правительства РФ от 16.03.2009 г. N 228: по сост. на 27 апреля 2017 г. // Собрание законодательства РФ. – 2009. – N 12. – Ст. 1431.

1.35. Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям: постановление Правительства РФ от 18.05.2009 г. N 424: по сост. на 29 апреля 2017 г. // Собрание законодательства РФ. – 2009. – N 21. – Ст. 2573.

1.36. О единой автоматизированной информационной системе Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих

идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено: постановление Правительства РФ от 26.10. 2012 г. N 1101: по сост. на 25 апреля 2017 г. // Собрание законодательства РФ. – 2012. – N 44. – Ст. 6044.

1.37. Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования: приказ Минкомсвязи РФ от 25.08.2009 N 104: по сост. на 15 апреля 2017 г. // Российская газета. – N 188. – 2009.

1.38. О Требованиях к технологическим, программным и лингвистическим средствам обеспечения пользования официальными сайтами федеральных органов исполнительной власти: приказ Минэкономразвития России от 16.11.2009 г. N 470: по сост. на 28 апреля 2017 г. // Российская газета. – N 15. – 2010.

1.39. Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования: приказ ФСБ РФ N 416, ФСТЭК РФ N 489 от 31.08.2010 г.: по сост. на 03 мая 2017 г. // Российская газета. – N 240. – 2010.

1.40. Об утверждении Положения об обработке персональных данных в центральном аппарате Министерства обороны Российской Федерации: приказ Министра обороны РФ от 16.06.2012 г. N 1500: по сост. на 23 апреля 2017 г. // Российская газета. – N 227. – 2012.

1.41. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России от 11.02.2013 г. N 17: по сост. на 06 мая 2017 г. // Российская газета. – N 136. – 2013.

1.42. Об утверждении Требований к технологическим, программным и лингвистическим средствам, необходимым для размещения информации государственными органами и органами местного самоуправления в сети «Интернет» в форме открытых данных, а также для обеспечения ее использования:

СТО БР ИББС-1.0-2014 «СТО БР ИББС-1.2-2014»: Стандарт Банка России от 17.05.2014 г. N Р-399: по сост. на 20 мая 2017 г. // Вестник Банка России. – N 48-49. – 2014.

1.48. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств «СТО БР ИББС-1.3-2016»: Стандарт Банка России от 30.11.2016 г. N ОД-4234: по сост. на 19 мая 2017 г. // Вестник Банка России. – N 107. – 2016.

1.49. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных: утв. ФСТЭК РФ от 14.02.2008 г. [Электронный ресурс]. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=77814/ (дата обращения 20.05. 2017 г.).

1.50. Положение о порядке создания, ведения и хранения баз данных на электронных носителях: утв. Банком России о 21.02.2013 г. N 397-П: по сост. на 23 мая 2017 г. // Вестник Банка России. – N 23. – 2013.

1.51. Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств: утв. Банком России от 09.06.2012 г. N 382-П: по сост. на 23 мая 2017 г. // Вестник Банка России. – N 32. – 2012.

1.52. Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности» РС БР ИББС-2.5-2014: введены в действие Распоряжением Банка России от 17.05.2014 г. N Р-400: по сост. на 16 мая 2017 г. // Вестник Банка России. – N 48-49. – 2014.

1.53. Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения

информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0» РС БР ИББС-2.0-2007: приняты и введены в действие Распоряжением Банка России от 28.04.2007 г. N Р-348: по сост. на 18 мая 2017 г. // Вестник Банка России. – N 29. – 2007.

1.54. Положение о Комитете Государственной Думы Федерального Собрания Российской Федерации по безопасности и противодействию коррупции утверждено решением Комитета Государственной Думы по безопасности и противодействию коррупции: протокол № 15/8, утверждено решением Комитета Государственной Думы по безопасности и противодействию коррупции от 17 января 2017 г. [Электронный ресурс]. URL: http://www.komitet2-16.km.duma.gov.ru/Polozhenie-i-voprosy-vedeniya/ (дата обращения 27.03. 2017 г.).

1.55. Положение о Департаменте информационных технологий, связи и защиты информации МВД России: приказ N 681, утверждено приказом МВД России от 16 июня 2011 г. [Электронный ресурс]. URL: https://мвд.рф/mvd/structure1/Departamenti/Departament_informacionnih_tehnologij_sv/Polozhenie/ (дата обращения 17.04. 2017 г.).

1.56. О рекомендациях по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности: письмо Банка России от 24.03.2014 г. N 49-Т: по сост. на 13 мая 2017 г. // Вестник Банка России. – N 34. – 2014.

2. Научная литература

2.1. Артамонова Я.С. Информационная безопасность российского общества: теоретические основания и практика политического обеспечения: автореферат дис. ... докт. полит. наук: 23.00.02 / Я.С. Артамонова. – МГОУ. –Москва, 2014. – 56 с.

2.2. Бачило И. Л. Информационное право: учебник / И. Л. Бачило. – 4-е изд., перераб. и доп. – М.: Издательство Юрайт, 2016. – 435с.

2.3. Булавин А.В. О подходах США и Китая к обеспечению кибербезопасности / А.В. Булавин // Общество: политика, экономика, право, 2014. – №1. – С.27-31.

2.4. Гольтяпина И.Ю. Административно-правовые средства обеспечения информационной безопасности в России: автореф. дис. ... канд. юрид. наук: 12.00.14 / И.Ю. Гольтяпина. – ОмГУ им. Ф.М. Достоевского. – Омск, 2008. – 26 с.

2.5. Козлов Д.Е. Влияние «вредной» информации на подростков / Д.Е. Козлов // Инновационные научные исследования: теория, методология, практика: сб. науч. ст. VIII Междунар. науч.–практич. конф., Пенза: Наука и Просвещение, 2017. – С. 207-209.

2.6. Кузнецов П.У. Основы информационного права учебник: для студентов высших учебных заведений / П.У. Кузнецов. – М.: Проспект, 2014. – 312с.

2.7. Левашов М. Стандарт Банка России или ГОСТ? Новые механизмы обеспечения информационной безопасности банков / М. Левашов // Бухгалтерия и банки, 2017. – N 1. – С. 62 - 63.

2.8. Лопатин В. Н. Информационная безопасность России: Человек, общество, государство / В. Н. Лопатин – М.: Безопасность человека и общества, 2000. – 428 с.

2.9. Молчанов Н.А., Матевосова Е.К. Доктрина информационной безопасности Российской Федерации (новелла законодательства) / Н.А. Молчанов, Е.К. Матевосова // Актуальные проблемы российского права, 2017. – N 2. – С. 159 - 165.

2.10. Основы управления информационной безопасностью. Учебное пособие для вузов / Курило А.П. [и др.]. –2-е изд., испр. –М.: Горячая линия–Телеком, 2016. –244 с.

2.11. Павлов И.Ю. Современные проблемы правового регулирования государственной и служебной тайны в России / И.Ю. Павлов // Ленинградский юридический журнал, 2013. – № 1 (31). – С. 29-37.

2.12. Петренко В.И. Теоретические основы защиты информации: учебное пособие / В.И. Петренко. – Ставрополь: Изд-во СКФУ, 2015. – 222 с.

2.13. Спектор Е.И. Комментарий к Закону Российской Федерации «О государственной тайне» (постатейный) / Е.И. Спектор. – М.: Юстицинформ, 2006. – 160 с.

2.14. Степанов-Егиянц В.Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации: монография / В.Г. Степанов-Егиянц. – М.: Статут, 2016. – 190 с.

2.15. Стрельцов А.А. Теоретические и методологические основы правового обеспечения информационной безопасности России: автореф. дис. ... докт. юрид. наук: 05.13.19 / А.А. Стрельцов. –МИФИ. – М. –2004. – 47 с.

2.16. Шариков П.А. Политика США в области информационной безопасности: дисс. ... канд. полит. наук: 23.00.04 / П.А Шариков. – Ин-т США и Канады РАН. – М. – 2009. – 216 с.

3. Интернет ресурсы

3.1. Восьмое управление Генерального штаба Вооруженных Сил Российской Федерации [Электронный ресурс] // Минобороны России: сайт. – URL:http://structure.mil.ru/structure/ministry_of_defence/details.htm?id=11159@egOrganization (дата обращения 12.05.2017 г.).

3.2. Глобальное исследование утечек конфиденциальной информации в 2016 году [Электронный ресурс] // Группа Компаний InfoWatch: сайт. – URL: https://www.infowatch.ru/report2016 (дата обращения 10.05.2017 г.).

3.3. Каталог пользователей ВКонтакте [Электронный ресурс] // сайт ВКонтакте: сайт. – URL: https://vk.com/catalog.php?selection=430-98 (дата обращения 03.05.2017 г.).

3.4. Лимиты: ограничения размеров операций [Электронный ресурс] // Яндекс.Денги: сайт. – URL: https://money.yandex.ru/page?id=523014 (дата обращения 26.05.2017 г.).

3.5. Массовые акции в Москве 6 мая 2012 года [Электронный ресурс] // РИА Новости: сайт. – URL: https://ria.ru/trend/moscow_meetings_06052012/ (дата обращения 07.05.2017 г.).

3.6. Псковские Бонни и Клайд: смерть в Интернете [Электронный ресурс] // Вести.ru: сайт. – URL: http://www.vesti.ru/doc.html?id=2821576 (дата обращения 18.05.2017 г.).

3.7. Развитие информационных угроз в первом квартале 2017 года. Статистика [Электронный ресурс] // АО «Лаборатория Касперского»: сайт. – URL: https://securelist.ru/analysis/malware-quarterly/30657/it-threat-evolution-q1-2017-statistics/ (дата обращения 16.05.2017 г.).

3.8. Управление «К» МВД России [Электронный ресурс] // МВД России: сайт. – URL: https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii (дата обращения 08.05.2017 г.).

3.9. About the Board [Электронный ресурс] // Privacy and Civil Liberties Oversight Board: сайт. – URL: https://www.pclob.gov/about-us.html (дата обращения 11.05.2017 г.).

3.10. About the Secret Service [Электронный ресурс] // The U.S. Secret Service: сайт. – URL: https://www.secretservice.gov/ (дата обращения 06.05.2017 г.).

3.11. Central Security Service [Электронный ресурс] // National Security Agency: сайт. – URL: https://www.nsa.gov/about/central-security-service/ (дата обращения 17.05.2017 г.).

3.12. Computer Fraud and Abuse Act of 1986 [Электронный ресурс] // Library of Congress: сайт. – URL: https://www.congress.gov/bill/99th-congress/house-bill/4718/text (дата обращения 11.04.2017 г.).

3.13. Constitution of the United States [Электронный ресурс] // United States Senate: сайт. – URL: https://www.senate.gov/civics/constitution_item/constitution (дата обращения 25.04.2017 г.).

3.14. Cybersecurity [Электронный ресурс] // United States Department of Homeland Security: сайт. – URL: https://www.dhs.gov/topic/cybersecurity (дата обращения 13.05.2017 г.).

3.15. Edward Snowden did enlist for special forces, US army confirms [Электронный ресурс] // The Guardian: сайт. – URL: https://www.theguardian.com/world/2013/jun/10/edward-snowden-army-special-forces (дата обращения 13.05.2017 г.).

3.16. EPIC v. NSA - Cybersecurity Authority [Электронный ресурс] // Electronic Privacy Information Center: сайт. – URL: https://epic.org/foia/nsa/nspd-54/default.html (дата обращения 16.04.2017 г.).

3.17. Financial Services Modernization Act of 1999 [Электронный ресурс] // U.S. Government Publishing Office: сайт. – URL: https://www.gpo.gov/fdsys/pkg/STATUTE-113/pdf/STATUTE-113-Pg1338.pdf (дата обращения 30.04.2017 г.).

3.18. Government organization and employees [Электронный ресурс] // U.S. Government Publishing Office: сайт. – URL: https://www.gpo.gov/fdsys/pkg/USCODE-2010-title5/html/USCODE-2010-title5-partI-chap5-subchapII-sec552a.htm (дата обращения 19.04.2017 г.).

3.19. Health Insurance Portability and Accountability Act of 1996 [Электронный ресурс] // U.S. Government Publishing Office: сайт. – URL: https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm (дата обращения 23.04.2017 г.).

3.20. Information Security Oversight Office (ISOO) [Электронный ресурс] // The U.S. National Archives and Records Administration: сайт. – URL: https://www.archives.gov/isoo (дата обращения 16.05.2017 г.).

3.21. Letting Your Kids Play in the Social Media Sandbox [Электронный ресурс] // The New York Times's: сайт. – URL: https://www.nytimes.com/2015/02/19/style/letting-your-kids-play-in-the-social-media-sandbox.html?_r=0 (дата обращения 23.04.2017 г.).

3.22. Mission & Strategy NSA [Электронный ресурс] // National Security Agency: сайт. – URL: https://www.nsa.gov/about/mission-strategy/ (дата обращения 18.05.2017 г.).

3.23. National Security Council [Электронный ресурс] // The White House President Donald J. Trump: сайт. – URL: https://www.whitehouse.gov/nsc/ (дата обращения 14.04.2017 г.).

3.24. National Security Telecommunications and Information Systems Security Committee (NSTISSC) [Электронный ресурс] // Committee national security systems: сайт. – URL: https://www.cnss.gov/ (дата обращения 03.05.2017 г.).

3.25. Obama Signs Last-Minute Patriot Act Extension [Электронный ресурс] // Fox News Politics: сайт. – URL: http://www.foxnews.com/politics/2011/05/27/senate-clearing-way-extend-patriot-act.html (дата обращения 18.04.2017 г.).

3.26. Obama to be urged to split cyberwar command from NSA [Электронный ресурс] // The Washington Post: сайт. – URL: https://www.washingtonpost.com/world/national-security/obama-to-be-urged-to-split-cyberwar-command-from-the-nsa/2016/09/12/0ad09a22-788f-11e6-ac8e-cf8e0dd91dc7_story.html?utm_term=.bdd8147f3173 (дата обращения 12.05.2017 г.).

3.27. Obar, Jonathan A.; Clement, Andrew (2013). «Internet Surveillance and Boomerang Routing: A Call for Canadian Network Sovereignty» [Электронный ресурс] // Proceedings of the Technology & Emerging Media Track – Annual Conference of the Canadian Communication Association. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2311792 (дата обращения 24.05.2017 г.).

3.28. Presidential Policy Directive 20 (PPD-20) [Электронный ресурс] // Federation of American Scientists: сайт. – URL: https://fas.org/irp/offdocs/ppd/ppd-20.pdf (дата обращения 05.04.2017 г.).

3.29. Privacy Act 1974 [Электронный ресурс] // U.S. Government Publishing Office: сайт. – URL: https://www.gpo.gov/fdsys/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf (дата обращения 20.04.2017 г.).

3.30. Securing cyberspace - President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts [Электронный ресурс] // The White House President Barack Obama https://obamawhitehouse.archives.gov/the-press-

office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat (дата обращения 09.04.2017 г.).

3.31. Senate approves USA Freedom Act [Электронный ресурс] // USA today: сайт. – URL: https://www.usatoday.com/story/news/politics/2015/06/02/patriot-act-usa-freedom-act-senate-vote/28345747/ (дата обращения 07.04.2017 г.).

3.32. The Bank Secrecy Act of 1970 [Электронный ресурс] // U.S. Government Publishing Office: сайт. – URL: https://www.gpo.gov/fdsys/pkg/STATUTE-84/pdf/STATUTE-84-Pg1114-2.pdf (дата обращения 13.04.2017 г.).

3.33. The Children's Online Privacy Protection Act of 1998 (COPPA) [Электронный ресурс] // U.S. Government Publishing Office: сайт. – URL: https://www.gpo.gov/fdsys/pkg/PLAW-105publ277/html/PLAW-105publ277.htm (дата обращения 19.04.2017 г.).

3.34. The Comprehensive National Cybersecurity Initiative [Электронный ресурс] // Federation of American Scientists: сайт. – URL: https://fas.org/irp/eprint/cnci.pdf (дата обращения 09.04.2017 г.).

3.35. The Confidential Information Protection and Statistical Efficiency Act of 2002 [Электронный ресурс] // Government library U.S.: сайт. – URL: https://www.eia.gov/cipsea/cipsea.pdf (дата обращения 15.04.2017 г.).

3.36. The Electronic Communications Privacy Act of 1986 (ECPA) [Электронный ресурс] // U.S. Government Publishing Office: сайт. – URL: https://www.gpo.gov/fdsys/pkg/STATUTE-100/pdf/STATUTE-100-Pg1848.pdf (дата обращения 18.04.2017 г.).

3.37. The Federal Information Security Management Act of 2002 [Электронный ресурс] // U.S. Government Publishing Office: сайт. – URL: http://www.gpo.gov/fdsys/pkg/STATUTE-116/pdf/STATUTE-116-Pg2899.pdf (дата обращения 27.04.2017 г.).

3.38. Traffic Overview vk.com [Электронный ресурс] // SimilarWeb: сайт. – URL: https://www.similarweb.com/website/vk.com#overview (дата обращения 03.05.2017 г.).

3.39. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001[Электронный ресурс] // U.S. Government Publishing Office: сайт. – URL: https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf (дата обращения 28.04.2017 г.).