НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «РОССИЙСКАЯ АКАДЕМИЯ АДВОКАТУРЫ И НОТАРИАТА»

Творческое задание

на тему: «Раскрытие понятие информационной безопасности»

Выполнил:
Магистрант 1 курса
Гайбулов Н.М.

Проверил:
_____

Москва, 2017

Актуальность выбранной темы находит свое отражение в широком развитие средств вычислительной техники и связи, что позволило собирать, хранить, обрабатывать и передавать информацию в таких объемах и с такой оперативностью, которые были немыслимы раньше.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

Под информационной безопасностью Российской Федерации[1] понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и

[1] Алексеев, В.М. Международные критерии оценки безопасности информационных технологий и их практическое применение: Учеб. пособие / В. М. Алексеев, В. В. Андрианов, С. Л. Зефиров ; М-во образования Рос. Федерации. Пенз. гос. ун-т. – Пенза: Изд-во Пенз. гос. ун-та, 2002

социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.[2]

На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.

Первая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Для достижения этого требуется:

повысить эффективность использования информационной инфраструктуры в интересах общественного развития, консолидации российского общества, духовного возрождения многонационального народа Российской Федерации;

усовершенствовать систему формирования, сохранения и рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала Российской Федерации;

обеспечить конституционные права и свободы человека и гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом, получать достоверную информацию о состоянии окружающей среды;

обеспечить конституционные права и свободы человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, на защиту своей чести и своего доброго Имени;

укрепить механизмы правового регулирования отношений в области охраны интеллектуальной собственности, создать условия для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации;

---

[2] Щербаков, А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. – М.: Книжный мир, 2009. – 352 с.

гарантировать свободу массовой информации и запрет цензуры; не допускать пропаганду и агитацию, которые способствуют разжиганию социальной, расовой, национальной или религиозной ненависти и вражды;

обеспечить запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен федеральным законодательством.

Вторая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Для достижения этого требуется:

укреплять государственные средства массовой информации, расширять их возможности по своевременному доведению достоверной информации до российских и иностранных граждан;

Третья составляющая национальных интересов Российской Федерации в информационной сфере включает в себя развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

Для достижения этого требуется:

развивать и совершенствовать инфраструктуру единого информационного пространства Российской Федерации;

развивать отечественную индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов;

развивать производство в Российской Федерации конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей этих средств и систем;

обеспечить государственную поддержку отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи.

интенсифицировать формирование открытых государственных информационных ресурсов, повысить эффективность их хозяйственного использования.

Четвертая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

В этих целях необходимо:

повысить безопасность информационных систем, включая сети связи, прежде всего безопасность первичных сетей связи и информационных систем федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами;

интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля за их эффективностью;

обеспечить защиту сведений, составляющих государственную тайну;
расширять международное сотрудничество Российской Федерации в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере.

Информационная безопасность включает[3]:

---

1. [3] Законодательные меры по борьбе с компьютерной преступностью // Проблемы преступности в капиталистических странах. М., 1988. № 10

- состояние защищенности информационного пространства, обеспечивающее его формирование и развитие в интересах граждан, организаций и государства;
- состояние инфраструктуры, при котором информация используется строго по назначению и не оказывает негативного воздействия на систему при ее использовании;
- состояние информации, при котором исключается или существенно затрудняется нарушение таких ее свойств, как конфиденциальность, целостность и доступность;
- экономическую составляющую (структуры управления в экономической сфере, включая системы сбора, накопления и обработки информации в интересах управления производственными структурами, системы общеэкономического анализа и прогнозирования хозяйственного развития, системы управления и координации в промышленности и на транспорте, системы управления энергосистем, централизованного снабжения, системы принятия решения и координации действий в чрезвычайных ситуациях, информационные и телекоммуникационные системы);
- финансовую составляющую (информационные сети и базы данных банков и банковских объединений, системы финансового обмена и финансовых расчетов).

Обеспечение информационной безопасности должно начинаться с выявления субъектов отношений, связанных с использованием информационных систем. Спектр их интересов может быть разделен на следующие основные категории: доступность (возможность за приемлемое время получить требуемую информационную услугу), целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения), конфиденциальность (защита от несанкционированного ознакомления).

В зависимости от способа воздействия на компьютерную систему специалисты выделяют четыре вида компьютерных преступлений[4]: ***Физические злоупотребления***, которые включают в себя разрушение оборудования; уничтожение данных или программ; ввод ложных данных, кражу информации, записанной на различных носителях. ***Операционные злоупотребления***, представляющие собой: мошенничество (выдача себя за другое лицо или использование прав другого лица); несанкционированное использование различных устройств. ***Программные***

[4] Ахраменка, Н.Ф. и др. Преступление и наказание в платежной системе с электронными документами// Управление защитой информации, 1998

злоупотребления, которые включают в себя: различные способы изменения системы математического обеспечения ("логическая бомба" - введение в программу команды компьютеру проделать в определенный момент какое-либо несанкционированное действие; "троянский конь" - включение в обычную программу своего задания). ***Электронные злоупотребления***, которые включают в себя схемные и аппаратные изменения, приводящие к тому же результату, что и изменение программы.

Российская действительность не является исключением и каждодневно приносит новые примеры преступлений в сфере информатизации и компьютеризации. Российский законодатель принял несколько срочных адекватных правовых мер противодействия этому новому виду преступности.

Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается или наказывается обществом, что так поступать не принято. В рамках обеспечения информационной безопасности следует рассмотреть на законодательном уровне две группы мер:

- меры, направленные на создание и поддержание в обществе негативного (в том числе карательного) отношения к нарушениям и нарушителям информационной безопасности;
- направляющие и координирующие меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности.

К первой группе следует отнести основные законодательные акты по информационной безопасности, являющиеся частью правовой системы Российской Федерации.

В Конституции РФ[5] содержится ряд правовых норм, определяющих основные права и свободы граждан России в области информатизации, в том числе ст. 23 определяет право на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений; ст. 42 обеспечивает право на получение достоверной информации о состоянии окружающей среды и др.

В Уголовном кодексе РФ имеются нормы, затрагивающие вопросы информационной безопасности граждан, организаций и государства.

---

[5] Конституция Российской Федерации" (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008

В числе таких статей ст. 137 «Нарушение неприкосновенности частной жизни», ст. 138 «Нарушение тайны переписки, телефонных переговоров, почтовых и телеграфных или иных сообщений», ст. 140 «Отказ в предоставлении гражданину информации», ст. 155 «Разглашение тайны усыновления (удочерения)», ст. 183 «Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну», ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование или распространение вредоносных программ для ЭВМ», ст. 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» и др.

В Налоговом кодексе РФ имеется ст. 102 «Налоговая тайна».

В Гражданском кодексе РФ вопросам обеспечения информационной безопасности посвящены ст. 139 «Служебная и коммерческая тайна», ст. 946 «Тайна страхования» и др.

Специальное законодательство в области информатизации и информационной безопасности включает ряд законов, и их представим в календарной последовательности.

С принятием в 1992 г. Закона Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных» впервые в России программное обеспечение компьютеров было законодательно защищено от незаконных действий. В том же году был принят Закон РФ «О правовой охране топологий интегральных микросхем».

Кодекс РФ об административных правонарушениях устанавливает ответственность за нарушение законодательства в области защиты информации.

Статья 13.12 предусматривает ответственность за нарушение правил защиты информации:

1. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), – влечет наложение административного штрафа на граждан в размере от 3 до 5 МРОТ; на должностных лиц – от 5 до 10 МРОТ; на юридических лиц – от 50 до 100 МРОТ.

2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), – влечет наложение административного штрафа на граждан в размере от 5 до 10 МРОТ с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц – от 10 до 20 МРОТ; на юридических

лиц – от 100 до 200 МРОТ с конфискацией несертифицированных средств защиты информации или без таковой.

3. Нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, – влечет наложение административного штрафа на должностных лиц в размере от 20 до 30 МРОТ; на юридических лиц – от 150 до 200 МРОТ.

4. Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, – влечет наложение административного штрафа на должностных лиц в размере от 30 до 40 МРОТ; на юридических лиц – от 200 до 300 МРОТ с конфискацией несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, или без таковой.

Статья 13.13 предусматривает ответственность за незаконную деятельность в области защиты информации.

1. Занятие видами деятельности в области защиты информации без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна), – влечет наложение административного штрафа на граждан в размере от 5 до 10 МРОТ с конфискацией средств защиты информации или без таковой; на должностных лиц – от 20 до 30 МРОТ с конфискацией средств защиты информации или без таковой; на юридических лиц – о 100 до 200 МРОТ с конфискацией средств защиты информации или без таковой.

2. Занятие видами деятельности, связанной с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну без лицензии, – влечет наложение административного штрафа на должностных лиц в размере от 40 до 50 МРОТ; на юридических лиц – от 300 до 400 МРОТ с конфискацией созданных без лицензии средств защиты информации, составляющей государственную тайну, или без таковой.

В 1993 г. принят Закон РФ «Об авторском праве и смежных правах», регулирующий отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства, фонограмм, исполнений и пр.

В 1993 г. был также принят Закон РФ «О государственной тайне»,

регулирующий отношения, возникающие в связи с отнесением сведений к государственной тайне.

В 1995 г. принят закон «О связи», регламентирующий на правовом уровне деятельности в области связи. Федеральный закон 1995 г. «Об информации, информатизации и защите информации» определяет ряд важных понятий таких, как информация, документ, информационные процессы, ресурсы и пр., а также регулирует отношения, возникающие при формировании и использовании информационных ресурсов, информационных технологий, защите информации и др. Правда, положения этого закона носят весьма общий характер, а основное содержание статей, посвященных информационной безопасности, сводится к необходимости использовать исключительно сертифицированные средства, что, в общем, правильно, но далеко не достаточно.

К группе направляющих и координирующих законов и нормативных актов относится целая группа документов, регламентирующих процессы лицензирования и сертификации в области информационной безопасности. Главная роль здесь отводилась Федеральному агентству правительственной связи и информации (ФАПСИ) и Государственной технической комиссии (Гостехкомиссии) при Президенте РФ.

В области информационной безопасности законы реально преломляются и работают через нормативные документы, подготовленные соответствующими ведомствами.

Самое важное на законодательном уровне – создать механизм, позволяющий согласовать процесс разработки законов с реалиями информационных технологий. Конечно, законы не могут опережать жизнь, но важно, чтобы отставание не было слишком большим, так как на практике, помимо прочих отрицательных моментов, это ведет к снижению информационной безопасности.

Неуклонный рост компьютерной преступности заставил законодателей России принять адекватные меры по борьбе с этим видом противоправных деяний, в т.ч. и уголовно-правовых. Главным является вступление в законную силу с 1 января 1997 г. нового Уголовного кодекса РФ, в который впервые включена глава «преступления в сфере компьютерной информации». Но начавшаяся работа нового УК РФ сразу же поставила ряд сложных вопросов перед наукой уголовного права и практикой ее применения. Нерешенные противоречия возникают при юридическом анализе преступлений в сфере компьютерной информации, а также во время проведения квалификации указанного вида преступлений.

Преступлениями в сфере компьютерной информации являются: неправомерный доступ к компьютерной информации (ст. 272 УК); создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК); нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети (274 УК).

Доктрина информационной безопасности Российской Федерации (далее – Доктрина) на период до 2020 года, утверждена Президентом РФ 24 июля 2013 г. Этот документ представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ (прил. №1).

Подводя итог о выделении информационной безопасности в качестве объекта уголовно-правовой охраны, полагаю необходимым выделение в Особенной части раздела "Преступления против информационной безопасности". Предвосхищая критические замечания о том, что это может нарушить систему Особенной части УК РФ

Составов преступлений, ответственность за которые предусмотрена нормами Особенной части УК РФ. Их также следует относить к посягательствам на информационную безопасность. В то же время эти нормы образуют самостоятельные институты, будучи объединены в соответствующие главы и разделы. Например, ст. 202 УК РФ предусматривает уголовную ответственность за злоупотребление полномочиями частными нотариусами и аудиторами. Разглашение нотариальной или аудиторской тайны этими лицами будет полностью охватываться диспозицией рассматриваемой статьи. Основным объектом в данном случае являются общественные отношения, обеспечивающие нормальный порядок службы в коммерческих и иных организациях, дополнительным же объектом будут являться общественные отношения, обеспечивающие безопасность личности в информационной сфере. Поэтому полагаю, что необходимо вести речь об информационной безопасности как объекте уголовно-правовой охраны и об информационной безопасности как о сложном институте уголовного права, который еще не сформирован. По моему мнению, процесс его формирования должен осуществляться параллельно с иными мерами, направленными на обеспечение безопасности в информационной сфере.

Очевидно, что Российской Федерации предстоит большая работа в этом направлении. Действующее уголовное законодательство не отвечает вышеназванным требованиям. Отсутствие единого четкого подхода к криминализации противоправных посягательств в информационной сфере, недооценка значимости уголовно-правовых средств в механизме правового

обеспечения информационной безопасности позволяют сделать вывод о том, что интересы личности, общества и государства в информационной сфере едва ли являются защищенными и над ними могут нависнуть серьезные угрозы.

Список литературы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008
2. Уголовный кодекс Российской федерации.
3. Автоматизированные информационные технологии в экономике: Учебник / Под ред. проф. Г.А. Титоренко. – М.: ЮНИТИ, 2000
4. Агеев, А. С., сост. Организация и современные методы защиты информации: Метод. пособие для рук. и сотрудников служб безопасности Агеев А. С. и др.; Под общ. ред. С. А. Диева, А. Г. Шаваева . – М.: Концерн"Банк. Деловой Центр", 1998
5. Аглицкий, И. Состояние и перспективы информационного обеспечения российских банков. – Банковские технологии, 1997
6. Аджиев, В. Мифы о безопасности программного обеспечения: уроки знаменитых катастроф. – Открытые системы, 199. №6
7. Алексеев, В.И. ,сост. Информационная безопасность муниципальных образований Учеб. пособие Ассоц. экон. взаимодействия обл. Центр.-Черноозем. региона Рос. Федерации "Черноземье" и др.; [Алексеев В. И. и др.]. – Воронеж: Изд-во Воронеж. гос. техн. ун-та, 1998
8. Алексеев, В.М. Международные критерии оценки безопасности информационных технологий и их практическое применение: Учеб. пособие / В. М. Алексеев, В. В. Андрианов, С. Л. Зефиров ; М-во образования Рос. Федерации. Пенз. гос. ун-т. – Пенза: Изд-во Пенз. гос. ун-та, 2002
9. Алексеев, В.М. Нормативное обеспечение защиты информации от несанкционированного доступа: Учеб. пособие В. М. Алексеев; М-во образования Рос. Федерации. Пенз. гос. ун-т. – Пенза: Изд-во Пенз. гос. ун-та, 2002
10. Алексеев, В.М. Обеспечение информационной безопасности при разработке программных средств: Учеб. пособие В.М. Алексеев, В.Г. Каминский, А.С. Овчаров; М-во общ. и проф образования Рос. Федерации. Пенз. гос. ун-т. – Пенза: Изд-во Пенз. гос. ун-та, 1999
11. Алешин, Л.И. Защита информации и информационная безопасность: Курс лекций Л. И. Алешин; Моск. гос. ун-т культуры. – М.: Моск. гос. ун-т культуры, 1999

12. Банки и банковские операции. Учебник / Под ред. Е.Ф. Жукова. – М.: Банки и биржи, ЮНИТИ, 1997
13. Ахраменка, Н.Ф. и др. Преступление и наказание в платежной системе с электронными документами// Управление защитой информации, 1998
14. Барсуков, В.С. Безопасность: технологии, средства, услуги. – М.: Кудиц – Образ, 2001
Батурин, Ю.М., Жодзишский, А.М. Компьютерная преступность и компьютерная безопасность. М.: Юр.лит., 1991
15. Бахметьев, А.В. Социальные факторы формирования информационного общества / Бахметьев А.В.; Ин-т социал.-полит. исслед. РАН, Фонд поддержки ученых "Науч. перспектива". – М.: Ин-т социал.-полит. исслед.: Фонд поддержки учен.
16. Безруков, Н.Н. Введение в компьютерную вирусологию. Общие принципы функционирования, классификация и каталог наиболее распространенных вирусов в М5-005. К., 1989
17. Безруков, Н.Н. Компьютерные вирусы. – М.: Наука, 2000
18. Белов, В.Н. Правонарушения, связанные с использованием ЭВМ // Проблемы совершенствования советского законодательства: Труды ВНИ-ИСЭ. Вып. 5. М., 1976
19. Бетелин, В.Б., ред. Вопросы кибернетики. Информационная безопасность. Операционные системы реального времени. Базы данных / Рос. акад. наук. Науч. совет по комплекс. пробл. "Кибернетика". Науч.-исслед. ин-т систем. исслед.; Под ред. В. Б. Бетелина. – М.: НИИ систем. исслед. РАН и др., 1999
20. Браун, С. "Мозаика" и "Всемирная паутина" для доступа к Internet: Пер. с англ. – М.: Мир: СК Пресс, 1999
21. Быков, В.А. Электронный бизнес и безопасность / В. А. Быков. – М.: Радио и связь, 2000
22. Законодательные меры по борьбе с компьютерной преступностью // Проблемы преступности в капиталистических странах. М., 1988. № 10

Приложение №1
к Творческому заданию
Магистра 1 курса Гайбулова Н.М.
на тему: Раскрытия понятия «Информационная безопасность»

Основы государственной политики российской Федерации в области международной информационной безопасности на период до 2020 года

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящие Основы являются документом стратегического планирования российской Федерации.

2. Настоящими Основами определяются основные угрозы в области международной информационной безопасности, цель, задачи и приоритетные направления государственной политики Российской Федерации в области международной информационной безопасности (далее — государственная политика Российской Федерации), а также механизмы их реализации.

3. Нормативную правовую базу настоящих Основ составляют Конституция Российской Федерации, международные договоры Российской Федерации в области международной информационной безопасности, федеральные законы, нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации, иные нормативные правовые акты Российской Федерации.

4. Настоящие Основы конкретизируют отдельные положения Стратегии национальной безопасности Российской Федерации до 2020 года, Доктрины информационной безопасности Российской Федерации, Концепции внешней политики Российской Федерации и других документов стратегического планирования Российской Федерации.

5. Настоящие Основы предназначены:

а) для продвижения на международной арене российских инициатив в области формирования системы международной информационной безопасности, включая совершенствование правового, организационного и иных видов ее обеспечения;

б) для формирования межгосударственных целевых программ в области Международной информационной безопасности, в осуществлении которых участвует Российская Федерация, а также государственных и федеральных целевых программ в данной области;

в) для организации межведомственного взаимодействия при реализации государственной политики Российской Федерации в области международной информационной безопасности;

г) для достижения и поддержания технологического паритета с ведущими мировыми державами за счет более широкого использования информационных и коммуникационных технологий в реальном секторе экономики.

6. Под международной информационной безопасностью понимается такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры.

7. Подсистемой международной информационной безопасности понимается совокупность международных и национальных институтов, призванных регулировать деятельность различных субъектов глобального информационного пространства.

Система международной информационной безопасности призвана оказать противодействие угрозам стратегической стабильности и способствовать равноправному стратегическому партнерству в глобальном информационном пространстве.

Сотрудничество в области формирования системы международной информационной безопасности отвечает национальным интересам Российской Федерации и способствует укреплению ее национальной безопасности.

8. Основной угрозой в области международной информационной безопасности является использование информационных и коммуникационных технологий:

а) в качестве информационного оружия в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

б) в террористических целях, в том числе для оказания деструктивного воздействия на элементы критической информационной инфраструктуры, а также для пропаганды терроризма и привлечения к террористической деятельности

новых сторонников;

в) для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию;

г) для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ.

11. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по формированию системы международной информационной безопасности на двустороннем, многостороннем, Региональном и глобальном уровнях, являются:

а) создание условий для продвижения на международной арене российской инициативы в необходимости разработки и принятия государствами — членами Организации Объединенных Наций Конвенции об обеспечении международной информационной безопасности;

б) содействие закреплению российских инициатив в области формирования системы международной информационной безопасности в итоговых документах, изданных по результатам работы Группы правительственных экспертов Организации Объединенных Наций по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, а также содействие выработке под эгидой Организации Объединенных Наций правил поведения в области обеспечения международной информационной безопасности, отвечающих национальным интересам Российской Федерации;

в) проведение на регулярной основе двусторонних и многосторонних экспертных консультаций, согласование позиций и планов действий с государствами — членами Шанхайской организации сотрудничества, государствами — участниками Содружества Независимых Государств, государствами — членами Организации Договора о коллективной безопасности, государствами — участниками БРИКС, странами — членами Азиатско-тихоокеанского экономического сотрудничества, странами — членами «Группы восьми», «Группы двадцати», другими

государствами и международными структурами в области международной информационной безопасности;

г) продвижение на международной арене российской инициативы в интернационализации управления информационно-телекоммуникационной сетью «Интернет» и увеличение в этом контексте роли Международного союза электросвязи;

д) организационно-штатное укрепление структурных подразделений федеральных органов исполнительной власти, участвующих в реализации государственной политики Российской Федерации, а также совершенствование координации деятельности федеральных органов исполнительной власти в данной области;

е) создание механизма участия российского экспертного сообщества в совершенствовании аналитического и научно-методического обеспечения продвижения российских инициатив в области формирования системы международной информационной безопасности;

ж) создание условий для заключения между Российской Федерацией и иностранными государствами международных договоров о сотрудничестве в области обеспечения международной информационной безопасности;

з) усиление взаимодействия в рамках Соглашения между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности и содействие расширению состава участников указанного Соглашения;

и) использование научного, исследовательского и экспертного потенциала Организации Объединенных Наций, других международных организаций для продвижения российских инициатив в области формирования системы международной информационной безопасности.

12. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по созданию условий, способствующих снижению риска использования информационных и коммуникационных технологий для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности, являются:

а) развитие диалога с заинтересованными государствами о национальных подходах к противодействию вызовам и угрозам, возникающим в связи с масштабным использованием информационных и коммуникационных технологий в военно-политических целях;

б) участие в выработке на двустороннем и многостороннем уровнях мер по укреплению доверия в области противодействия угрозам использования информационных и коммуникационных технологий для осуществления враждебных действий и актов агрессии;

в) содействие развитию региональных систем и формированию глобальной системы международной информационной безопасности на основе общепризнанных принципов и норм международного права (уважение государственного суверенитета, невмешательство во внутренние дела других государств, неприменение силы и угрозы силой в международных отношениях, право на индивидуальную и коллективную самооборону, уважение прав и основных свобод человека);

г) содействие подготовке и принятию государствами — членами Организации Объединенных Наций международных правовых актов, регламентирующих применение принципов и норм международного гуманитарного права в сфере использования информационных и коммуникационных технологий;

д) создание условий для установления международного правового режима нераспространения информационного оружия.

13. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по формированию механизмов международного сотрудничества в области противодействия угрозам использования информационных и коммуникационных технологий в террористических целях, являются:

а) развитие сотрудничества с государствами — членами Шанхайской организации сотрудничества, государствами — участниками Содружества Независимых Государств, государствами — членами Организации Договора о коллективной безопасности, государствами — участниками БРИКС, способствующего предупреждению, выявлению, пресечению, раскрытию и расследованию актов Деструктивного воздействия на элементы национальной критической информационной инфраструктуры, минимизации последствий реализации таких актов, а также противодействию использования информационно-телекоммуникационной сети «Интернет» и других информационно-телекоммуникационных сетей в Целях пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

б) содействие подготовке и принятию государствами — членами Организации Объединенных Наций акта, определяющего порядок обмена информацией о передовых практиках в области обеспечения безопасности функционировали элементов критической информационной инфраструктуры.

14. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по созданию условий для противодействия угрозам использования информационных и коммуникационных технологий в экстремистских целях, в том числе в целях вмешательства во внутренние дела суверенных государств, являются:

а) участие в разработке и реализации межгосударственной системы мер по противодействию указанным угрозам;

б) содействие созданию международного механизма постоянного контроля за недопущением использования информационных и коммуникационных технологий в экстремистских целях, в том числе в целях вмешательства во внутренние дела суверенных государств.

15. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по повышению эффективности международного сотрудничества в области противодействия преступности в сфере использования информационных и коммуникационных технологий, являются:

а) продвижение на международной арене российской инициативы в необходимости разработки и принятия под эгидой Организации Объединенных Наций Конвенции о сотрудничестве в сфере противодействия информационной преступности, а также активизация работы с государствами — членами Шанхайской организации сотрудничества, государствами — участниками Содружества

Независимых Государств, государствами — членами Организации Договора о коллективной безопасности, государствами — участниками БРИКС по поддержке данной инициативы;

б) развитие сотрудничества в сфере противодействия информационной преступности с государствами — членами Шанхайской организации сотрудничества, государствами — участниками Содружества Независимых Государств, государствами — членами Организации Договора о коллективной безопасности, государствами — участниками БРИКС, странами -членами Азиатско-тихоокеанского экономического сотрудничества, странами — членами «Группы восьми», «Группы двадцати», другими государствами и международными структурами;

в) повышение эффективности информационного обмена между правоохранительными органами государств в ходе расследования преступлений в сфере использования информационных и коммуникационных технологий;

г) совершенствование механизма обмена информацией о методиках расследования и судебной практике рассмотрения дел о преступлениях в сфере использования информационных и коммуникационных технологий.

16. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по созданию условий для обеспечения технологического суверенитета государств в области информационных и коммуникационных технологий и преодоления информационного неравенства между развитыми и развивающимися странами, являются:

а) содействие разработке и реализации международных программ, способствующих преодолению информационного неравенства между развитыми и развивающимися странами;

б) содействие развитию национальных информационных инфраструктур и участию государств мирового сообщества в процессах создания и использования глобальных информационных сетей и систем.

17. Государственная политика Российской Федерации реализуется федеральными органами исполнительной власти и надзорными органами в соответствии с предметами их ведения при выполнении соответствующих межгосударственных целевых программ, в осуществлении которых участвует Российская федерация, государственных и федеральных целевых программ, в том числе в рамках государственно-частного партнерства.

18. Подготовка предложений Президенту Российской Федерации по реализации основных направлений государственной политики Российской

Федерации осуществляется рабочими органами Совета Безопасности Российской Федерации во взаимодействии с заинтересованными самостоятельными подразделениями Администрации Президента Российской Федерации, федеральными органами исполнительной власти и организациями.

19. Общая координация деятельности федеральных органов исполнительной власти, связанной с реализацией государственной политики Российской Федерации, а также с продвижением согласованной позиции Российской Федерации по этому вопросу на международной арене, осуществляется Министерством иностранных дел Российской Федерации.

***

20. Интенсивное развитие информационных и коммуникационных технологий, их широкое применение во всех сферах деятельности человека создали Условия для формирования глобальной информационной инфраструктуры, которая предоставила качественно новые возможности социализации людей, их общения и доступа к накопленным человечеством знаниям.

В современном обществе информационные и коммуникационные технологи являются основным фактором, определяющим уровень социально-экономического развития и состояние национальной безопасности.

Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года призваны способствовать активизации внешней политики Российской Федерации на пути достижения согласия и учета взаимных интересов в процессе интернационализации глобального информационного пространства.

Конвенция об обеспечении международной информационной безопасности (концепция)

ПРЕАМБУЛА

Государства-участники настоящей Конвенции, отмечая значительный прогресс в развитии информационно-коммуникационных технологий и средств, формирующих информационное пространство, выражая озабоченность угрозами, связанными с возможностями использования таких технологий и средств в целях, не совместимых с задачами

обеспечения международной безопасности и стабильности, как в гражданской, так и в военной сферах,

придавая важное значение международной информационной безопасности как одному из ключевых элементов системы международной безопасности, будучи убежденными в том, что дальнейшее углубление доверия и развитие взаимодействия государств-участников в вопросах обеспечения международной информационной безопасности являются настоятельной необходимостью и отвечают их интересам,

принимая во внимание важное значение информационной безопасности для реализации основных прав и свобод человека и гражданина,