МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное
учреждение высшего образования
«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ РАДИОЭЛЕКТРОНИКИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Кафедра «Информационная безопасность»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОВРЕМЕННОМ МИРЕ

Учебно-методическое пособие
для обучающихся по направлению
10.03.01 «Информационная безопасность»
очной и очно-заочной форм обучения

Севастополь
СевГУ
2022

УДК 004.056(075.8)
ББК 16.8я73
И74

Р е ц е н з е н т :
Ю.Ю. Гончаренко – д-р техн. наук, профессор,
профессор кафедры «Информационная безопасность»

Составитель: Е.А. Контылева

И74 **Информационная безопасность в современном мире**: учебно-методическое пособие для обучающихся по направлению 10.03.01 «Информационная безопасность» очной и очно-заочной форм обучения / Севастопольский государственный университет, Институт радиоэлектроники и информационной безопасности, кафедра «Информационная безопасность» ; сост. Е.А. Контылева. – Севастополь : СевГУ, 2022. – 68 с. – Текст: электронный.

В данном учебно-методическом пособии рассмотрены основные средства защиты информации, структуры и организации, отвечающие за ИБ, методы и средства ведения информационной войны. Частично раскрыты основные пункты концепции и доктрины ИБ.

Данное пособие может быть использовано для самостоятельной подготовки и выполнения лабораторных работ студентов очной и очно-заочной форм обучения - направления подготовки 10.03.01 «Информационная безопасность».

УДК 004.056(075.8)
ББК 16.8я73

Рассмотрено и утверждено на заседании кафедры «Информационная безопасность», протокол № 8 от 18 февраля 2022 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Учебная дисциплина «Информационная безопасность в современном мире» включает в себя теоретические аспекты обеспечения информационной безопасности в современном мире. Основная цель этой дисциплины заключается в формировании системы знаний об информационной безопасности общества, организации, государства и основных мерах по её обеспечению. Дисциплина носит междисциплинарный характер и тесно связана с другими дисциплинами специальности «Информационная безопасность».

Предполагается, что в результате изучения этой дисциплины студенты получат знания:

- о современных средствах обработки и систематизации информации;
- правил работы в коллективе.

Будут владеть:

– навыками быстро ориентироваться в современных средствах обработки информации;

– навыками коммуникации для решения профессиональных задач.

Успешно изучившие данную дисциплину будут уметь:

– успешно использоваться современные средства обработки информации для решения профессиональных задач;

– организовать взаимодействие коллег в вопросах информационной безопасности.

1. СТРУКТУРЫ И ОРГАНИЗАЦИИ, ОТВЕЧАЮЩИЕ ЗА ИБ

Согласно Доктрине информационная безопасность РФ может быть обеспечена комплексными методами и средствами.

Комплексное обеспечение ИБ — это взаимосвязанный комплекс правовых, организационных, физических, социальных, духовных, информационных, программно-математических и технических методов, мероприятий и средств, обеспечивающих нормальное функционирование государства, его структур, населения, фирм, предприятий как на его территории и в его пространстве, так и в межгосударственных отношениях, независимо от состояний государства — мирного труда или военного времени.

Методологию комплексного обеспечения ИБ определяет государственная политика РФ в этом направлении.

Государственная политика обеспечения ИБ РФ определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов РФ в этой области, порядок закрепления их обязанностей по защите интересов РФ в информационной сфере в рамках направлений их деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

Государственная политика обеспечения ИБ основывается на следующих основных принципах:

- соблюдение Конституции РФ, законодательства РФ, общепризнанных принципов и норм международного права;
- открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов РФ и общественных объединений, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством РФ;
- правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса;
- приоритетное развитие отечественных современных информационных и телекоммуникационных технологий.

Государство в процессе реализации своих функций по обеспечению ИБ в Российской Федерации:

- проводит объективный и всесторонний анализ и прогнозирование угроз ИБ в Российской Федерации, разрабатывает меры по ее обеспечению;
- организует работу законодательных (представительных) и исполнительных органов государственной власти Российской Федерации по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз ИБ;

- поддерживает деятельность общественных объединений, направленную на объективное информирование населения о социально значимых явлениях общественной жизни, защиту общества от искаженной и недостоверной информации;
- осуществляет контроль за разработкой, созданием, развитием, использованием, экспортом и импортом средств защиты информации посредством их сертификации и лицензирования деятельности в области защиты информации;
- проводит необходимую протекционистскую политику в отношении производителей средств информатизации и защиты информации на территории Российской Федерации и принимает меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;
- способствует предоставлению физическим и юридическим лицам доступа к мировым информационным ресурсам, глобальным информационным сетям;
- формулирует и реализует государственную информационную политику России;
- организует разработку федеральной программы обеспечения ИБ РФ, объединяющей усилия государственных и негосударственных организаций в данной области;
- способствует интернационализации глобальных информационных сетей и систем, а также вхождению России в мировое информационное сообщество на условиях равноправного партнерства.

Основными *элементами* организационной основы государственной системы обеспечения ИБ РФ являются: Президент РФ, Совет безопасности РФ, Совет Федерации Федерального Собрания РФ, Государственная Дума Федерального Собрания РФ, Правительство РФ, федеральные органы исполнительной власти, межведомственные и государственные комиссии, создаваемые Президентом РФ и Правительством РФ, органы исполнительной власти субъектов РФ, органы местного самоуправления, органы судебной власти, общественные объединения, граждане, принимающие в соответствии с законодательством РФ участие в решении задач обеспечения ИБ РФ.

Президент РФ руководит в пределах своих конституционных полномочий органами и силами по обеспечению ИБ РФ, санкционирует действия по обеспечению ИБ РФ; в соответствии с законодательством РФ формирует, реорганизует и упраздняет подчиненные ему органы и силы по обеспечению ИБ РФ; определяет в своих ежегодных посланиях Федеральному Собранию РФ приоритетные направления государственной политики в области обеспечения ИБ РФ, а также меры по реализации Доктрины ИБ РФ.

Совет безопасности РФ является конституционным совещательным органом, непосредственно занимающимся вопросами государственной безопасности. Совет безопасности РФ проводит работу по выявлению и

оценке угроз ИБ РФ, оперативно подготавливает проекты решений Президента РФ по предотвращению таких угроз, разрабатывает предложения в области обеспечения ИБ РФ, а также предложения по уточнению отдельных положений Доктрины, координирует деятельность органов и сил по обеспечению ИБ РФ, контролирует реализацию федеральными органами исполнительной власти и органами исполнительной власти субъектов РФ решений Президента РФ в этой области. В его состав входит Межведомственная комиссия по ИБ, которая готовит указы Президента РФ, выступает с законодательной инициативой в области ИБ государства.

Правительство РФ в пределах своих полномочий и с учетом сформулированных в ежегодных посланиях Президента РФ Федеральному Собранию РФ приоритетных направлений в области обеспечения ИБ РФ координирует деятельность федеральных органов исполнительной власти и органов исполнительной власти субъектов РФ, а также при формировании в установленном порядке проектов федерального бюджета на соответствующие годы предусматривает выделение средств, необходимых для реализации федеральных программ в этой области. Федеральные министерства и ведомства могут в своем составе создавать соответствующие службы и подразделения для решения вопросов обеспечения ИБ на отраслевом уровне.

Межведомственные и государственные комиссии, создаваемые Президентом РФ и Правительством РФ, решают в соответствии с предоставленными им полномочиями задачи обеспечения ИБ РФ. На Межведомственную комиссию по защите государственной тайны возложена задача координации действий государственных структур по вопросам зашиты информации.

Рабочим органом Межведомственной комиссии является Федеральная служба по техническому и экспертному контролю (в недавнем прошлом эта структура называлась Государственной технической комиссией при Президенте РФ), которая:

- разрабатывает стратегию и определяет приоритетные направления деятельности по обеспечению безопасности информации;
- осуществляет подготовку проектов законов, разрабатывает нормативные документы по ИБ;
- контролирует эффективность защиты информации в ключевых системах информационной инфраструктуры, в информационных системах и объектах, на которых выполняются работы, связанные со сведениями, составляющими государственную и (или) служебную тайну;
- проводит лицензирование деятельности по осуществлению мероприятий и оказанию услуг в области технической защиты государственной тайны, по разработке и производству средств защиты информации;
- организует проведение работ по сертификации средств технической защиты информации, безопасности информационных технологий;

- организует разработку и согласование федеральных целевых программ обеспечения безопасности информации, технической защиты информации, защиты государственной тайны;
- организует разработку программ стандартизации, технических регламентов и национальных стандартов в области ИБ;
- организует проведение межведомственных экспертиз реального уровня безопасности информации.

Федеральная служба безопасности РФ является федеральным органом исполнительной власти, осуществляющим государственное управление в области обеспечения безопасности РФ, борьбе с терроризмом, защиты и охраны Государственной границы, обеспечивающим информационную безопасность РФ и другие функции, определенные законодательством РФ. При ФСБ действует Институт криптографии, связи и информатики (ИКСИ).

Основными *задачами ФСБ* с точки зрения защиты информации являются:

- обеспечение защиты сведений, составляющих государственную тайну;
- противодействие иностранным техническим разведкам;
- организация обеспечения криптографической и инженерно-технической безопасности инфотелекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи;
- разработка и производство шифров и ключевых документов к шифровальным средствам;
- разработка и реализация мер по защите сведений, составляющих государственную тайну, в федеральных органах государственной власти, органах власти субъектов РФ, воинских формированиях и организациях;
- осуществление мер, связанных с допуском граждан к сведениям, составляющим государственную тайну;
- разработка и утверждение нормативных и методических документов по вопросам обеспечения ИБ инфотелекоммуникационных систем и др.

Федеральная служба охраны РФ является федеральным органом исполнительной власти, осуществляющим функции по выработке

государственной политики, нормативно-правовому регулированию, контролю и надзору в сфере государственной тайны, президентской, правительственной и иных видов специальной связи и информации, предоставляемых федеральным органам государственной власти, органам государственной власти субъектов РФ и другим государственным органам.

Основными *задачами ФСО* с точки зрения защиты информации являются:

- разработка и реализация единой технической политики в области оснащения Администрации Президента РФ, Аппарата Правительства РФ и палат Федерального Собрания РФ средствами открытой и специальной связи, вычислительной техникой, аудио- и видеоаппаратурой, программными продуктами;

- организация и обеспечение эксплуатации, безопасности, совершенствования специальной связи и информации, предоставляемых государственным органам, обеспечение защиты категорированных помещений, проведение специальных исследований и проверок технических средств связи и дополнительного оборудования;
- участие в разработке и реализации мер по обеспечению ИБ РФ, противодействию техническим разведкам и защите сведений, составляющих государственную тайну;
- разработка, создание и развитие средств защиты информации, специальных технических средств, а также разработка нормативнотехнической документации по вопросам защиты информации в системах специальной связи;
- осуществление функций удостоверяющего центра в информационных системах, ведение реестра сертификатов ключей для цифровых подписей уполномоченных лиц федеральных органов государственной власти и др.

Служба внешней разведки РФ является составной частью сил обеспечения безопасности и защиты безопасности личности, общества и государства от внешних угроз.

Основными *задачами СВР с* точки зрения защиты информации являются:

- допуск предприятий к проведению работ, связанных с использованием сведений, составляющих государственную тайну (за рубежом);
- участие в проведении работ, связанных с созданием средств ЗИ;
- осуществление мероприятий и оказание услуг в области защиты государственной тайны;
- участие в лицензионной деятельности в области ЗИ и др.

Палаты Федерального Собрания РФ на основе Конституции РФ по представлению Президента РФ и Правительства РФ формируют законодательную базу в области обеспечения ИБ РФ. Совет Федерации имеет Комитет по обороне и безопасности. В составе Государственной Думы имеется Комитет по безопасности.

Следующим уровнем в системе обеспечения ИБ являются органы исполнительной власти субъектов РФ, органы местного самоуправления, которые могут также создавать различные комиссии. Органы исполнительной власти субъектов РФ взаимодействуют с федеральными органами исполнительной власти по вопросам исполнения законодательства РФ, решений Президента РФ и Правительства РФ в области обеспечения ИБ РФ. а также по вопросам реализации федеральных программ в этой области; совместно с органами местного самоуправления осуществляют мероприятия по привлечению граждан, организаций и общественных объединений к оказанию содействия в решении проблем обеспечения ИБ РФ; вносят в

федеральные органы исполнительной власти предложения по совершенствованию системы обеспечения ИБ РФ.

Контролирующими и правоохранительными органами федерального уровня, обеспечивающими соблюдение нормативно-правовых норм, являются; Конституционный Суд РФ, Верховный Суд РФ, Генеральная прокуратура РФ.

Нижним уровнем системы обеспечения ИБ являются структурные подразделения и должностные лица предприятий и организаций.

Структура государственных органов обеспечения ИБ в РФ показана на рис. 1.1

Технологическими мероприятиями комплексной системы обеспечения ИБ в нашем государстве являются:

- разработка нормативной правовой базы в области обеспечения ИБ РФ;
- создание условий для реализации прав граждан и общественных объединений на разрешенную законодательством РФ деятельность в информационной сфере;
- определение и поддержание баланса между потребностью граждан, общества и государства в свободном обмене информацией и необходимыми ограничениями на распространение информации;
- оценка состояния ИБ РФ, выявление источников внутренних и внешних угроз ИБ, определение приоритетных направлений предотвращения, отражения и нейтрализации этих угроз;
- координация деятельности федеральных органов государственной власти и других государственных органов, решающих задачи обеспечения ИБ РФ;
- контроль деятельности федеральных органов государственной власти и органов государственной власти субъектов РФ. государственных и межведомственных комиссий, участвующих в решении задач обеспечения ИБ РФ;
- предупреждение, выявление и пресечение правонарушений, связанных с посягательствами на законные интересы граждан, общества и государства в информационной сфере, на осуществление судопроизводства по делам о преступлениях в этой области;
- развитие отечественной информационной инфраструктуры, а также индустрии телекоммуникационных и информационных средств;
- повышение конкурентоспособности информационных средств на внутреннем и внешнем рынках;
- организация разработки федеральной и региональных программ обеспечения ИБ и координация деятельности по их реализации;
- проведение единой технической политики в области обеспечения ИБ РФ;
- организация фундаментальных и прикладных научных исследований в области обеспечения ИБ РФ;

- защита государственных информационных ресурсов, прежде всего в федеральных органах государственной власти и органах государственной власти субъектов РФ, на предприятиях оборонного комплекса;
- обеспечение контроля над созданием и использованием средств защиты информации посредством обязательного лицензирования деятельности в данной сфере и сертификации средств защиты информации;
- совершенствование и развитие единой системы подготовки кадров, используемых в области ИБ РФ;
- осуществление международного сотрудничества в сфере обеспечения ИБ, представление интересов РФ в соответствующих международных организациях.

Рис. 1.1. Структура государственных органов обеспечения ИБ в Российской Федерации

2. СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Средства защиты информации – это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

В соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 для обеспечения защиты информации, содержащейся в государственных информационных системах, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. N 184-ФЗ "О техническом регулировании"

Средства защиты информации принято делить на нормативные (неформальные) и технические (формальные).

Неформальными средствами защиты информации – являются нормативные (законодательные), административные (организационные) и морально-этические средства, к которым можно отнести: документы, правила, мероприятия.

Правовую основу (законодательные средства) информационной безопасности обеспечивает государство. Защита информации регулируется международными конвенциями, Конституцией, федеральными законами «Об информации, информационных технологиях и о защите информации», законы Российской Федерации «О безопасности», «О связи», «О государственной тайне» и различными подзаконными актами.

Не соблюдение данных законов влечет за собой угрозы информационной безопасности, которые могут привести к значительным последствиям, что в свою очередь наказуемо в соответствии с этими законами в плоть до уголовной ответственности.

Административные (организационные) мероприятия играют существенную роль в создании надежного механизма защиты информации. Так как возможности несанкционированного использования конфиденциальных сведений в значительной мере обусловливаются не техническими аспектами, а злоумышленными действиями. Например нерадивостью, небрежностью и халатностью пользователей или персонала защиты.

Для снижения влияния этих аспектов необходима совокупность организационно-правовых и организационно-технических мероприятий, которые исключали бы или сводили к минимуму возможность возникновения угроз конфиденциальной информации.

В данной административно-организационной деятельности по защите информационной для сотрудников служб безопасности открывается простор для творчества.

Это и архитектурно-планировочные решения, позволяющие защитить переговорные комнаты и кабинеты руководства от прослушивания, и установление различных уровней доступа к информации.

С точки зрения регламентации деятельности персонала важным станет оформление системы запросов на допуск к интернету, внешней электронной почте, другим ресурсам. Отдельным элементом станет получение электронной цифровой подписи для усиления безопасности финансовой и другой информации, которую передают государственным органам по каналам электронной почты.

К морально-этическим средствам можно отнести сложившиеся в обществе или данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение их приравнивается к несоблюдению правил поведения в обществе или коллективе. Эти нормы не являются обязательными, как законодательно утвержденные нормы, однако, их несоблюдение ведет к падению авторитета, престижа человека или организации.

В целом средства обеспечения защиты информации в части предотвращения преднамеренных действий в зависимости от способа реализации можно разделить на группы:

Технические (аппаратные) средства. Это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации. Они либо препятствуют физическому проникновению, либо, если проникновение все же состоялось, доступу к информации, в том числе с помощью ее маскировки. Первую часть задачи решают замки, решетки на окнах, защитная сигнализация и др. Вторую — генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные каналы утечки информации или позволяющих их обнаружить. Преимущества технических средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. Слабые стороны — недостаточная гибкость, относительно большие объем и масса, высокая стоимость.

Программные средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств — универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки — ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).

Смешанные аппаратно-программные средства реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства.

Организационные средства складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых (национальные законодательства и правила работы, устанавливаемые руководством конкретного предприятия). Преимущества организационных средств состоят в том, что они позволяют решать множество разнородных проблем, просты в реализации, быстро реагируют на нежелательные действия в сети, имеют неограниченные возможности модификации и развития. Недостатки — высокая зависимость от субъективных факторов, в том числе от общей организации работы в конкретном подразделении.

По степени распространения и доступности выделяются программные средства, другие средства применяются в тех случаях, когда требуется обеспечить дополнительный уровень защиты информации.

3. РОЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБЕСПЕЧЕНИИ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

Под системой национальной безопасности или системой обеспечения национальной безопасности (СОНБ) понимается совокупность органов, сил и средств. Она является многоуровневой и предполагает взаимодействие государственных органов, общественных институтов, бизнеса и граждан с целью сохранения суверенитета страны, предотвращения посягательств на ее интересы, сбережения национального богатства. Реализуется система внутри страны, во взаимодействии между регионами и в рамках международных отношений, предполагая одновременную и в равной степени защиту интересов государства, общества и личности.

Информационная безопасность в системе занимает одну из ведущих позиций ролей. В России принимаются основополагающие документы в наиболее важных сферах жизнеобеспечения страны. Разработана и действует Доктрина информационной безопасности, ставшая краеугольным камнем в разработке современной системы защиты от цифровых угроз. Она дала определение информационной сферы, в которой должны применяться внедряемые взгляды на безопасность.

Доктрина информационной безопасности.

Вторая редакция Доктрины была принята в 2016 году, до этого действовал более ранний документ 2000 года. Она разработана Советом Безопасности РФ и стала теоретической и концептуальной основой для создания нормативно-правовых актов и внедрения проектов, целью которых стала защита интересов России от кибератак и иных цифровых угроз.

Угрозы прямо названы в документе:

- рост научного и технического потенциала ряда государств, стремящихся закрепить свой приоритет на международной арене и использующих для этого информационные ресурсы. Используются такие методы, как прямое цифровое вторжение в инфраструктуру жизнеобеспечения и применение ресурсов научно-технической разведки;
- усиление информационно-психологического воздействия на население, использование информационных технологий для изменения менталитета и поведения граждан;
- использование технологий цифровых атак и хакерского потенциала экстремистскими и террористическими группировками, национальными и международными;
- возрастание масштабов кибератак на объекты инфраструктуры, финансовую сферу, бизнес и граждан;
- недостаточный уровень развития собственного научного и кадрового потенциала.

Фиксация угроз привела к реализации проектов национального масштаба, призванных минимизировать риски, возникающие в сфере

информационной безопасности как неотъемлемой составляющей национальной безопасности.

Деятельность государства в области информационной безопасности.

Защита суверенитета государства в цифровом мире требует существенных усилий. Роль государства в усилении информационной безопасности в системе национальной безопасности выражается в следующих направлениях:

- нормативно-правовое регулирование на законодательном и подзаконном уровнях;
- реализация национальных проектов;
- регулирование на уровне исполнительной власти;
- организация взаимодействия государства и общества.

Если регулирование и взаимодействие носят системный и непрерывный характер, то национальные проекты направлены на прорывное решение наиболее значимых задач.

«Цифровая экономика»

Национальный проект «Цифровая экономика», реализуемый Министерством цифрового развития, связи и массовых коммуникаций РФ, предусматривает выполнение нескольких подпрограмм:

1. Кадры.
2. Безопасность.
3. Технологии.
4. Государственное управление.

Их реализация рассчитана на период до 2024 года. В рамках подпроекта «Информационная безопасность» планируется решить ключевые задачи, призванные обеспечить устойчивое развитие национальной информационной инфраструктуры, подготовку кадров и развитие технологий, повысить экспортный потенциал отрасли, гарантировать полную защиту интересов государства и общества.

На период реализации программы предусмотрено:

- предоставить поддержку 100 экспортно-ориентированным компаниям, что должно обеспечить устойчивое присутствие национальных информационных технологий на международной арене;
- добиться маршрутизации на территории России не менее 90 % сетевого трафика (концепция суверенного Рунета);
- обеспечить использование не менее чем 97 % населения средств защиты информации;
- снизить долю иностранного программного обеспечения, покупаемого или арендуемого государственными организациями, до 10 % в структуре общей цены закупок.

В рамках подпроекта с осени 2019 года началось предоставление субсидий ряду исполнителей. На его реализацию до 2024 года планируется затратить 167 миллиардов рублей.

Среди показателей в цифровом выражении, которых предполагается достичь к 2024 году:

- снизить среднее время простоев ГИС (государственных информационных систем) в результате информационных атак с 65 часов на конец 2018 года до 1 часа в 2024 году, что должно сыграть ключевую роль в сфере защиты информации;
- повысить процент населения, применяющего отечественные средства защиты информации, с 86 % до 97 %;
- повысить количество специалистов, подготовленных по направлению защиты информации, с 7 до 24 тысяч;
- снизить долю иностранного ПО в общей цене закупок ПО государственными органами и компаниями с 50 % до 10 %.

Помимо показателей, которых планируется достичь, определены конкретные действия, которые уже достигнуты и должны быть реализованы в рамках нацпроекта:

1. Предполагается, что безопасность информационного пространства и сети Интернета недостаточно отрегулирована на уровне международного права, отсутствуют документы, которые позволяют устранить перевес сил в пользу отдельных государств. В рамках решения этой задачи в международные организации (ООН) внесены проекты соглашений и конвенций, направленных на реализацию принципа паритетности в сфере информационных технологий, равного участия государств в управлении Интернетом. Так, Россия стала инициатором первой резолюции Генеральной Ассамблеи ООН о «Достижениях в области информатизации и телекоммуникаций в контексте международной безопасности в 1998 году» и намерена продолжить движение в этом направлении.

2. Нападения иностранных хакеров на сети электрообеспечения страны признаны одной из основных угроз национальной и экономической безопасности. Были проанализированы угрозы, составлена их модель и внесены предложения по изменению отраслевых стандартов и нормативно-правовых актов с целью создания единой устойчивой системы защиты объектов электросистемы, принадлежащих различным собственникам, что усложняет задачу создания единого пространства регулирования системы защиты от сетевых атак.

3. Обеспечение информационной безопасности требует преимущественной маршрутизации трафика в пределах границ Российской Федерации. Разработаны концепция и основные нормативные акты в направлении создания суверенного Рунета, началось их внедрение. Правовой статус российского сегмента Интернета законодательно закреплен.

4. От устойчивости сетей связи зависит качество управления и взаимодействия государственных органов. Были законодательно закреплены требования к устойчивости и безопасности сетей связи и оборудования как для ГИС, так и для компаний различных организационно-правовых форм.

5. Сети общего пользования могут стать объектами направленных атак. Разработана и внедряется система мониторинга состояния сетей общего пользования. Изменены требования к проектированию сетей связи общего пользования с учетом действующей модели угроз. Новые общие и частные сети могут создаваться только при условии их соответствия разработанным параметрам.

6. Информационная безопасность призвана решать задачи обеспечения правопорядка. Разработан и внедряется комплекс решений по внедрению отечественных информационных технологий при реализации программы «Умный город».

Среди уже внедренных проектов, обеспечивающих защиту интересов государства и общества, особое значение имеет ГосСОПКА – государственный центр обнаружения и предотвращения компьютерных атак. Его поддержкой занимается ФСБ РФ, на ведомство ложатся ключевые задачи обеспечения национальной безопасности в информационной сфере.

ГосСОПКА

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы, созданная по указу президента РФ № 620, предназначена для решения четырех основных задач в сфере информационной безопасности как части национальной безопасности:

- прогнозирование рисков атак в информационном пространстве;
- взаимодействие между собой и с государством компаний, которым принадлежат значимые информационные ресурсы, особенно обслуживающие критические объекты инфраструктуры, для выявления, предупреждения и ликвидации последствий цифровых атак;
- контроль и мониторинг уровня защищенности инфраструктуры от цифровых атак;
- расследование инцидентов информационной безопасности.

За общее рабочее состояние системы отвечает ФСБ РФ. Все организации любой формы собственности, имеющие в распоряжении объекты критической информационной инфраструктуры (КИИ), обязаны создать у себя центры ГосСОПКА и оборудовать их в соответствии с требованиями ФСБ и ФСТЭК РФ. Отказ от выполнения этих требований, ввиду их важности для жизнеобеспечения страны и создания необходимого уровня информационной безопасности в системе национальной безопасности, предусматривает ответственность вплоть до уголовной.

С точки зрения информационной архитектуры ГосСОПКА выглядит как единый, но территориально распределенный комплекс центров управления и мониторинга, обменивающихся между собой информацией о кибератаках. Задача системы – объединение критически важной инфраструктуры в единую сеть с целью обмена информацией о кибератаках. Если такая атака совершается на один из объектов, он передает ее параметры

другим, и те имеют возможность подготовиться к нападению. Совместная система предупреждения уже доказала свою эффективность.

Система состоит из центров трех уровней – федерального, регионального и местного, в которые делятся на территориальные, ведомственные и корпоративные центры. Для борьбы с компьютерными атаками все они должны иметь следующие программные и аппаратные средства:

- обнаружения. Средства выявляют не инциденты, а именно значимые события информационной безопасности, чаще всего они реализуются по модели SIEM;
- предупреждения. Механизм предупреждения, инвентаризации и мониторинга реализуется программными средствами класса Vulnerability Scanner или сканерами защищенности. В большинстве компаний с КИИ такие средства уже внедрены согласно рекомендациям ФСТЭК РФ;
- ликвидации последствий. Здесь реализуется совместная работа участников системы над ликвидацией последствий компьютерных атак, реализуемая в виде Incident Response Platform;
- расшифровки;
- обмена информацией;
- криптографической защиты каналов связи, в данном случае дополнительной разработки средств шифрования именно для ГосСОПКИ не потребовалось.

Разработка программных средств для их внедрения в центрах ГосСОПКА ведется крупнейшими компаниями – производителями программного обеспечения в стране, что является одним из проявлений взаимодействия государства и общества в сфере информационной безопасности как части национальной безопасности.

Зона совместного регулирования

Государство уполномочено принимать нормативные акты и рекомендации в сфере обеспечения компьютерной безопасности, но они непосредственно влияют на общество и бизнес, вынуждая корректировать планы и бюджеты. Современная концепция взаимодействия власти и общества в сфере информационной безопасности предполагает, что практически все нормативные акты, существенно затрагивающие общественные интересы, должны пройти стадию предварительного общественного обсуждения.

Особенно это касается значимых законопроектов. Так, законопроект о суверенном Рунете проходил длительное общественное обсуждение, пока не были учтены основные замечания. Это же касается ряда рекомендаций ФСТЭК РФ, относящихся к сертификации программного обеспечения, ведомство прислушивается к аргументам бизнеса и вносит корректировки в свои проекты. Невозможно решать вопросы такого уровня, как ограничение пользования Интернетом, без учета интересов личности, поэтому в обсуждении концепции цифровой безопасности принимали участие не

только Ростелеком и «Лаборатория Касперского», но и общественность. Законопроект был размещен опубликован в Интернете для открытого обсуждения, что позволило скорректировать ряд направлений государственной политики, так как состояние информационной защищенности гражданина предполагает и его информированность о тех действиях государства, которые могут повлиять на его поведение.

Международно-правовое взаимодействие государства и общества

Государство не может действовать в одиночку, ему нужно стабильное взаимодействие с институтами гражданского общества и бизнесом, это позволяет достичь синергии в создании информационной безопасности в системе национальной безопасности РФ. Крупнейшие производители компьютерных технологий понимают, что в современном мире силовой инструментарий государства зачастую стоит на службе у крупных корпораций, и кибероружие иностранных государств во многом будет задействовано против российского бизнеса. Так, в начале 2019 года Франция приняла новую доктрину кибербезопасности, разрешающую «превентивные кибератаки», тем самым признав факт разработки кибероружия. Она оказалась не первой, ранее факт таких разработок признавал Китай.

Исходя из представленного Минкомсвязи паспорта проекта «Информационная безопасность», критическая инфраструктура пока не готова к целенаправленному отражению массированной атаки на системы жизнеобеспечения, энергосеть, крупнейшие промышленные предприятия. Бизнес полностью готов к сотрудничеству с государством, видя общую опасность. Наиболее существенной проблемой видится возможность внешнего проникновения в системы АСУ предприятий. Евгений Касперский утверждает, что в 2018 году такие попытки осуществлялись в отношении 48 % систем АСУ. Это побуждает к выработке новых защитных решений, авария на нефтепроводе способна полностью парализовать регион. Это побуждает бизнес в защите своих интересов активнее включаться в общегосударственную работу в области информационной безопасности.

На сегодня частно-государственное взаимодействие в области кибербезопасности развивается в различных направлениях. Несмотря на режим санкций, идет активное общение между учеными и предпринимателями России и стран Европы. Общество стремительно реализует модель «сетевой дипломатии», в которой бизнесмены нашей и зарубежных стран активно договариваются о создании кодекса этики, в рамках которого информационные атаки на экономическую инфраструктуру окажутся неприемлемым и не признаваемым экономическим сообществом мира методом конкурентной борьбы.

Риск киберинцидентов, инспирируемых международными террористическими группировками и опасных для общества и бизнеса, привел к возникновению компьютерных групп реагирования на чрезвычайные ситуации и команд компьютерной безопасности по реагированию на инциденты (CERTs / CSIRTs). Глобальный форум по

управлению Интернетом в 2017 году показал, что корпоративные CERTs из различных стран активно идут на сотрудничество друг с другом, выстраивая собственную трансграничную систему взаимодействия и ассистируя борьбе государств с глобальными компьютерными угрозами. В России участником глобального тренда стал RU-CERT – российский центр реагирования на компьютерные инциденты.

Бизнес выдвигает идеи создания некой общей среды кибербезопасности, в которой реализовывались бы переплетенные интересы государства и общества. Так, в октябре 2019 года состоялось заседание Клуба «Безопасность информации в промышленности», в котором приняли участие лидеры бизнеса России – «Норникель», «Северсталь», «Лукойл», «Юнипро», «Газпром нефть», «Фосагро», «НЛМК». Примером такого взаимодействия стало рассмотрение на международном уровне разработанной компанией «Норникель» Хартии информационной безопасности критических объектов промышленности в ОБСЕ и в Совет Баренцева/Евроарктического региона.

Признаваемая потенциальными участниками Хартии информационная безопасность в системе национальной безопасности выступает гарантом отказа не только бизнеса, но и государств от конфликтов с использованием кибероружия, последствия которых могут оказаться критическими. Хартия «Норникеля» осуждает использование информационных технологий в целях недобросовестной конкуренции и нанесения ущерба объектам промышленности и «приветствует усилия международного сообщества по приданию опорным информационно-коммуникационным инфраструктурам, формирующим основу глобальной сети, статуса демилитаризованной зоны, свободной от силового противоборства политических субъектов».

Этот документ не единственный, бизнес уже несколько лет выступает с инициативами усилить совместное регулирование борьбы с кибероружием:

- Microsoft в 2014 году предложил Цифровую Женевскую конвенцию, включающую шесть основных принципов международной кибербезопасности, применимых в мирное время. Компания потребовала от государств ограничить гонку кибервооружений;
- Соглашение о кибербезопасности (предложено Cybersecurity Tech Accord в 2018 году);
- Хартия доверия Siemens (Charter of Trust), также 2018 год. Компания сформулировала основные принципы организации совместной политики кибербезопасности;
- два документа предложила в этом же году Глобальная комиссия по киберстабильности (GCCS), они касаются защиты «публичного ядра» Интернета и обеспечения безопасности инфраструктуры, используемой для проведения выборов и референдумов.

Пока ни один из названных документов не вышел из стадии обсуждения, это касается и схожих документов в сфере международного права, предлагаемых иными международными субъектами.

4. КОНЦЕПЦИЯ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В Концепции информационной безопасности Российской Федерации (далее — Концепция) на основе анализа современного состояния информационной безопасности определены цели, задачи и ключевые проблемы обеспечения информационной безопасности.

Рассмотрены объекты, угрозы информационной безопасности и возможные их последствия, методы и средства предотвращения, парирования и нейтрализации угроз, а также особенности обеспечения информационной безопасности в различных сферах деятельности государства.

Излагаются основные положения государственной политики обеспечения информационной безопасности в Российской Федерации, организационная структура и принципы построения системы информационной безопасности.

Концепция служит методологической основой разработки комплекса нормативно-правовых и организационно-методических документов, регламентирующих деятельность в области информационной безопасности органов представительной, исполнительной и судебной властей Российской Федерации, субъектов Российской Федерации, органов местного самоуправления (далее — органы государственной власти и управления), предприятий, учреждений и организаций независимо от их организационно-правовой формы и формы собственности (далее — предприятия).

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение, правовая основа Концепции информационной безопасности Российской Федерации

Концепция информационной безопасности Российской Федерации представляет собой официально принятую систему взглядов на проблему обеспечения информационной безопасности, методы и средства защиты жизненно важных интересов личности, общества, государства в информационной сфере.

Концепция является составной частью Концепции национальной безопасности Российской Федерации и служит методологической основой:

- разработки стратегии обеспечения информационной безопасности страны, включающей в себя цели, задачи и комплекс основных мер по ее практической реализации;
- формирования и проведения государственной политики Российской Федерации в области обеспечения информационной безопасности;
- подготовки предложений по совершенствованию правового, нормативно-методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;
- разработки целевых программ защиты информационных ресурсов и средств информатизации.

Положения Концепции должны учитываться при формировании государственной политики информатизации, создания и развития единого информационного пространства России.

Правовую основу Концепции составляют Конституция Российской Федерации, законы Российской Федерации "О безопасности", "О государственной тайне", "Об информации, информатизации и защите информации", другие законодательные акты Российской Федерации, а также международные договоры и соглашения, заключенные или признанные Российской Федерацией, определяющие права и ответственность граждан, общества и государства в информационной сфере.

1.2. Роль и место информационной безопасности в общей системе национальной безопасности Российской Федерации.

Информационная безопасность играет ключевую роль в обеспечении Жизненно важных интересов Российской Федерации. Это, в первую очередь, обусловлено насущной потребностью, создания развитой и защищенной информационной среды общества. Именно через информационную среду осуществляются угрозы национальной безопасности в различных сферах деятельности государства.

В политической сфере все большее значение приобретают информационные факторы. В традиционном противостоянии политических соперников растут удельный вес и значимость информационно-психологического воздействия.

Экономический потенциал государства все в большей степени определяется объемом информационных ресурсов и уровнем развития информационной инфраструктуры. В то же время растет уязвимость экономических структур от недостоверности, запаздывания и незаконного использования экономической информации.

В военной сфере исход вооружённой борьбы все в большей степени зависит от качества добываемой информации и уровня развития информационных технологий, на которых основываются системы разведки, радиоэлектронной борьбы, управления войсками и высокоточным оружием.

В сфере духовной жизни возникает опасность развития в обществе агрессивной потребительской идеологии, тотальной коммерциализации культуры, распространения идей насилия и нетерпимости, воздействия на психику разрушительных форм мифологизированного сознания. Эти угрозы и защита от них, а также утверждение нравственных ценностей реализуются внутри информационной среды и прежде всего через средства массовой информации и формирования общественного мнения.

Информационная среда, являясь системообразующим фактором во всех сферах национальной безопасности, активно влияет на состояние политической, экономической, оборонной и других составляющих национальной безопасности Российской Федерации. В то же время она представляет собой самостоятельную сферу национальной безопасности, в которой необходимо обеспечить защиту информационных ресурсов, систем

их формирования, распространения и использования, информационной инфраструктуры, реализацию прав на информацию государства, юридических лиц, граждан.

1.3. Основные цели и задачи обеспечения информационной безопасности Российской Федерации

Основные цели обеспечения информационной безопасности определяются на базе устойчивых приоритетов национальной безопасности, отвечающих долговременным интересам общественного развития, к которым относятся:

- сохранение и укрепление российской государственности и политической стабильности в обществе;
- сохранение и развитие демократических институтов общества, обеспечение прав и свобод граждан, укрепление законности и правопорядка;
- обеспечение достойной роли России в мировом сообществе;
- обеспечение территориальной целостности страны;
- обеспечение прогрессивного социально-экономического развития России;
- сохранение национальных культурных ценностей и традиций.

В соответствии с указанными приоритетами основными целями информационной безопасности являются:

- защита национальных интересов России в условиях глобализации информационных процессов, формирования мировых информационных сетей и стремления США и других развитых стран к информационному доминированию;
- обеспечение органов государственной власти и управления, предприятий и граждан достоверной, полной и своевременной информацией, необходимой для принятия решений, а также предотвращение нарушений целостности и незаконного использования информационных ресурсов;
- реализация прав граждан, организаций и государства на получение, распространение и использование информации.

К основным задачам обеспечения информационной безопасности относятся:

- выявление, оценка и прогнозирование источников угроз информационной безопасности;
- разработка государственной политики обеспечения информационной безопасности, комплекса мероприятий и механизмов ее реализации;
- разработка нормативно-правовой базы обеспечения информационной безопасности, координация деятельности органов государственной власти и управления и предприятий по обеспечению информационной безопасности;
- развитие системы обеспечения информационной безопасности, совершенствование ее организации, форм, методов и средств предотвращения, парирования и нейтрализации угроз информационной безопасности и ликвидации последствий ее нарушения;

- обеспечение активного участия России в процессах создания и использования глобальных информационных сетей и систем.

1.4. Объекты информационной безопасности Российской Федерации

К объектам информационной безопасности Российской Федерации относятся:

- информационные ресурсы, вне зависимости от форм хранения, содержащие информацию, составляющую государственную тайну и ограниченного доступа, коммерческую тайну и другую конфиденциальную информацию, а также открытую (общедоступную) информацию и знания;

- система формирования, распространения и использования информационных ресурсов, включающая в себя информационные системы различного класса и назначения, библиотеки, архивы, базы и банки данных, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, научно-технический и обслуживающий персонал;

- информационная инфраструктура, включающая центры обработки и анализа информации, каналы информационного обмена и телекоммуникации, механизмы обеспечения функционирования телекоммуникационных систем и сетей, в том числе системы и средства защиты информации;

- система формирования общественного сознания (мировоззрение, политические взгляды, моральные ценности и пр.), базирующаяся на средствах массовой информацией пропаганды;

- права граждан, юридических лиц и государства на получение, распространение и использование информации, защиту конфиденциальной информации и интеллектуальной собственности.

Информационная безопасность всех вышеуказанных объектов создает условия надежного функционирования государственных и общественных институтов, а также формирования общественного сознания, отвечающего прогрессивному развитию страны.

II. АНАЛИЗ СОСТОЯНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

2.1. Основные факторы, влияющие на состояние информационной безопасности Российской Федерации

Происходящие в настоящее время процессы преобразования в политической жизни и экономике России оказывают непосредственное влияние на состояние ее информационной безопасности. При этом возникают новые факторы, которые необходимо учитывать при оценке реального состояния информационной безопасности и определении ключевых проблем в этой области.

Указанные факторы можно разделить на политические, экономические и организационно-технические.

Политическими факторами являются:

- изменение геополитической обстановки вследствие фундаментальных перемен в различных регионах мира, сведения к минимуму вероятности мировой ядерной и обычной войн;

- информационная экспансия США и других развитых стран, осуществляющих глобальный мониторинг мировых политических, экономических, военных, экологических и других процессов, распространяющих информацию в целях получения односторонних преимуществ;

- становление новой российской государственности на основе принципов демократии, законности, информационной открытости;

- разрушение ранее существовавшей командно-административной системы государственного управления, а также сложившейся системы обеспечения безопасности страны;

- нарушение информационных связей вследствие образования независимых государств на территории бывшего СССР;

- стремление России к более тесному сотрудничеству с зарубежными странами в процессе проведения реформ на основе максимальной открытости сторон;

- низкая общая правовая и информационная культура в российском обществе.

Среди экономических факторов наиболее существенными являются: переход России на рыночные отношения в экономике, появление множества отечественных и зарубежных коммерческих структур — производителей и потребителей информации, средств информатизации и защиты информации, включение информационной продукции в систему товарных отношений;

- критическое состояние отечественных отраслей промышленности, производящих средства информатизации и защиты информации;

- расширяющаяся кооперация с зарубежными странами в развитии информационной инфраструктуры России.

Из организационно-технических факторов определяющими являются:

- недостаточная нормативно-правовая база в сфере информационных отношений, в том числе в области обеспечения информационной безопасности;

- слабое регулирование государством процессов функционирования и развития рынка средств информатизации, информационных продуктов и услуг в России;

- широкое использование в сфере государственного управления и кредитно-финансовой сфере незащищенных от утечки информации импортных технических и программных средств для хранения, обработки и передачи информации;

- рост объемов информации, передаваемой по открытым каналам связи, в том числе по сетям передачи данных и межмашинного обмена;

- обострение криминогенной обстановки, рост числа компьютерных преступлений, особенно в кредитно-финансовой сфере.

2.2. Оценка состояния и ключевые проблемы обеспечения информационной безопасности Российской Федерации

За последние годы в Российской Федерации реализован комплекс практических мер по совершенствованию информационной безопасности.

Начато формирование нормативно-правового обеспечения информационной безопасности. Приняты законы Российской Федерации "О государственной тайне", "Об информации, информатизации и защите информации", развернуты работы по созданию механизмов их реализации, завершена подготовка ряда законопроектов, регламентирующих деятельность \S субъектов в информационной сфере. Осуществлен ряд практических мероприятий по совершенствованию информационной безопасности в органах государственной власти и управления и на предприятиях. Успешному решению ряда вопросов информационной безопасности способствует создание Государственной системы защиты информации и системы лицензирования деятельности предприятий в области защиты информации.

Вместе с тем, анализ современного состояния информационной безопасности в России показывает, что уровень информационной безопасности в настоящее время не соответствует жизненно важным потребностям личности, общества и государства.

Сегодняшние условия политического и социально-экономического развития страны вызывают обострение противоречий между потребностями об щества в расширении свободного обмена информацией и необходимостью сохранения отдельных ограничений на ее распространение.

Отсутствие действенных механизмов регулирования информационных отношений в обществе и государстве приводит ко многим негативным последствиям.

Слабое обеспечение органов государственной власти и управления полной, достоверной и своевременной информацией затрудняет принятие обоснованных решений. Неразвитость информационных отношений в сфере предпринимательства тормозит становление цивилизованного рынка. Отсутствие механизма включения информационного ресурса в хозяйственный оборот приводит к серьезным экономическим потерям.

Недостаточная защищенность государственного информационного ресурса приводит к утрате важной политической, экономической и научно-технической информации, в том числе о новых и высокоэффективных технологиях военного и двойного назначения.

Необеспеченность прав граждан на информацию, манипулирование информацией вызывает неадекватную реакцию населения и в ряде случаев ведет к политической нестабильности в обществе.

Потерям важной информации способствуют бессистемность защиты данных и слабая координация мер по защите информации в общегосударственном масштабе, ведомственная разобщенность в обеспечении целостности и конфиденциальности «информации, слабый

контроль за экспортом отечественных наукоемких технологий, образцов вооружения и военной техники.

Неблагоприятно обстоят дела с охраной государственной тайны. Серьезно ослаблены меры по обеспечению сохранности государственных секретов, коммерческой и служебной тайны в органах государственной власти и управления и на предприятиях оборонного комплекса.

Гарантированные Конституцией Российской Федерации основные права и свободы, такие как право на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, практически не имеют правового, организационного и технического обеспечения. Неудовлетворительно организована защита персональных данных, налоговой, таможенной, имущественной и другой информации.

Продолжается спад производства на государственных предприятиях, в том числе специализирующихся на выпуске защищенной техники, предназначенной для обработки секретной информации. Разрушаются научные и производственные коллективы, наблюдается массовый уход в коммерческие структуры наиболее квалифицированных кадров.

Отставание отечественных информационных технологий вынуждает массового потребителя идти по пути закупок незащищенной импортной техники, в результате чего повышается вероятность несанкционированного доступа к базам и банкам данных, а также возрастает зависимость страны от иностранных производителей компьютерной и телекоммуникационной Техники и информационной продукции.

Такое положение дел в области обеспечения информационной безопасности не позволяет России на равноправной основе включиться в мировую информационную систему и требует безотлагательного решения следующих ключевых проблем:

1. Развития научно-практических основ информационной безопасности, отвечающей современной геополитической ситуации и условиям политического и социально-экономического развития Российской Федерации.

2. Формирования законодательной и нормативно-правовой базы обеспечения информационной безопасности, в том числе разработка реестра информационного ресурса, регламента информационного обмена для органов государственной власти и управления, предприятий, нормативного закрепления ответственности должностных лиц и граждан за соблюдение требований информационной безопасности.

3. Разработки механизмов реализации прав граждан на информацию.

4. Формирования системы информационной безопасности, обеспечивающей реализацию государственной политики в области информационной безопасности.

5. Разработки современных методов и технических средств, обеспечивающих комплексное решение задач защиты информации.

6. Разработки критериев и методов оценки эффективности систем и средств информационной безопасности и их сертификации.

7. Исследований форм и способов цивилизованного воздействия государства на формирование общественного сознания.

8. Комплексного исследования деятельности персонала информационных систем, в том числе методов повышения мотивации, морально-психологической устойчивости и социальной защищенности людей, работающих с секретной и конфиденциальной информацией.

III. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

3.1. Источники угроз информационной безопасности Российской федерации

Источники угроз информационной безопасности в Российской Федерации можно разделить на внешние и внутренние. К внешним источникам относятся:

- недружественная политика иностранных государств в области глобального информационного мониторинга, распространения информации и новых информационных технологий;
- деятельность иностранных разведывательных и специальных служб;
- деятельность иностранных политических и экономических структур, направленная против интересов Российского государства;
- преступные действия международных групп, формирований и отдельных лиц;
- стихийные бедствия и катастрофы. Внутренними источниками угроз являются:
- противозаконная деятельность политических и экономических структур в области формирования, распространения и использования информации;
- неправомерные действия государственных структур, приводящие к Нарушению законных прав граждан и организаций в информационной сфере;
- нарушения установленных регламентов сбора, обработки и передачи информации;
- преднамеренные действия и непреднамеренные ошибки персонала информационных систем;
- отказы технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах.

3.2. Способы воздействия угроз на объекты информационной безопасности Российской Федерации

Способы воздействия угроз на объекты информационной безопасности в Российской Федерации подразделяются на информационные, программно-математические, физические, радиоэлектронные, организационно-правовые.

К информационным способам относятся:

- нарушения адресности и своевременности информационного обмена, противозаконный сбор и использование информации;

- несанкционированный доступ к информационным ресурсам;

- манипулирование информацией (дезинформация, сокрытие или искажение информации);

- незаконное копирование данных в информационных системах;

- использование средств массовой информации с позиций, противоречащих интересам граждан, организаций и государства;

- хищение информации из библиотек, архивов, банков и баз данных;

- нарушение технологии обработки информации.

Программно-математические способы включают:

- внедрение программ-вирусов;

- установку программных и аппаратных закладных устройств; уничтожение или модификацию данных в информационных системах. Физические способы включают:

- уничтожение или разрушение средств обработки информации и связи;

- уничтожение, разрушение или хищение машинных или других оригиналов носителей информации;

- хищение программных или аппаратных ключей и средств криптографической защиты информации;

- воздействие на персонал;

- поставка "зараженных" компонентов информационных систем.

Радиоэлектронными способами являются:

- перехват информации в технических каналах ее утечки;

- внедрение электронных устройств перехвата информации в технических средствах и помещениях;

- перехват, дешифрование и навязывание ложной информации в сетях передачи данных и линиях связи;

- воздействие на парольно-ключевые системы;

- радиоэлектронное подавление линий связи и систем управления.

Организационно-правовые способы включают:

- закупки несовершенных или устаревших информационных технологий и средств информатизации;

- невыполнение требований законодательства и задержки в принятии необходимых нормативно-правовых положений в информационной сфере;

- неправомерное ограничение доступа к документам, содержащим важную для граждан и организаций информацию.

3.3. Возможные последствия воздействия угроз информационной безопасности Российской Федерации

В результате воздействия угроз информационной безопасности может быть нанесен серьезный ущерб жизненно важным интересам Российской Федерации в политической, экономической, оборонной и других сферах деятельности государства, причинен социально-экономический ущерб обществу и отдельным гражданам.

Вследствие такого воздействия могут быть созданы препятствия на пути равноправного сотрудничества России с развитыми странами и

дружественными государствами, затруднено принятие важнейших политических, экономических и других решений, подорван государственный авторитет Российской Федерации на международной арене, создана атмосфера напряженности и политической нестабильности в обществе, нарушен баланс интересов личности, общества и государства, дискредитированы органы государственной власти и управления, спровоцированы социальные, национальные и религиозные конфликты, инициированы забастовки и массовые беспорядки, нарушено функционирование системы государственного управления, а также систем управления войсками, вооружением и военной техникой, объектами повышенной опасности.

Следствием воздействия угроз могут явиться снижение темпов научно-технического развития страны, утрата культурного наследия, проявления бездуховности и безнравственности.

Весьма существенный экономический ущерб в различных областях общественной жизни и в сфере бизнеса может быть причинен в результате нарушений законодательства в информационной сфере и компьютерных преступлений,

Угрозы информационной безопасности могут нанести физический, материальный и моральный ущерб гражданам, вызывать неадекватное социальное и криминальное поведение групп людей или отдельных лиц, оказать влияние на процессы образования и формирования личности.

IV. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

4.1. Базовые методы предотвращения, парирования и нейтрализации угроз информационной безопасности Российской Федерации

В целях предотвращения, парирования и нейтрализации угроз информационной безопасности применяются правовые, программно-технические и организационно-экономические методы.

Правовые методы предусматривают разработку комплекса нормативно-правовых актов и положений, регламентирующих информационные отношения в обществе, руководящих и нормативно-методических документов по обеспечению информационной безопасности.

Программно-технические методы включают предотвращение утечки обрабатываемой информации путем исключения несанкционированного доступа К ней, предотвращение специальных воздействий, вызывающих разрушение; уничтожение, искажение информации или сбои в работе средств информатизации, выявление внедренных программных или аппаратных закладных устройств, исключение перехвата информации техническими средствами, применения криптографических средств защиты информации при передаче по каналам связи.

Организационно-экономические методы предусматривают формирование и обеспечение функционирования систем защиты секретной и конфиденциальной информации, сертификации этих систем по требованиям информационной безопасности, лицензирования деятельности в сфере информационной безопасности, стандартизации способов и средств защиты информации, контроль за действием персонала в защищенных информационных системах.

Важное место среди этих методов занимают мотивация; экономическое стимулирование и психологическая поддержка деятельности персонала, занятого обеспечением информационной безопасности.

4.2. Особенности обеспечения информационной безопасности в различных сферах, деятельности государства и общегосударственных информационных и телекоммуникационных системах

Рассмотренные выше объекты, угрозы, методы и средства обеспечения информационной безопасности являются общими для различных сфер деятельности государства.

Вместе с тем, в каждой из этих сфер имеются свои особенности обеспечения информационной безопасности, что в первую очередь связано со спецификой решения поставленных задач, наличием свойственных каждой области информационной безопасности слабых элементов и уязвимых звеньев.

Поэтому в каждой сфере деятельности государства требуется специальная организация работ, использование форм и способов обеспечения информационной безопасности с учетом специфических факторов, влияющих на ее состояние.

В политической сфере

Наиболее серьезной опасности в политической сфере подвергаются:

- общественное сознание и политическая ориентация различных групп населения страны (регионов), непрерывно формируемые под воздействием отечественных и зарубежных средств массовой информации (печать, радио, телевидение);

- система принятия политических решений, существенно зависящая от качества и своевременности ее информационного обеспечения;

- права политических организаций, партий, объединений и движений на закрепленное в Конституций Российской Федерации свободное выражение своих программ, социально-политических и экономических ориентации через средства массовой информации;

- система регулярного информирования населения органами государственной власти и управления о политической и социально-экономической жизни через средства массовой информации, пресс-центры, центры общественных связей и т.п.;

- система формирования общественного мнения, включающая специальные институты, центры и службы выявления, изучения и анализа общественного мнения.

Для демократического развития страны наибольшую опасность представляют следующие угрозы:

- односторонняя политическая ориентация средств массовой информации под давлением государственных органов, господствующих политических сил, а также под экономическим давлением отдельных групп, в том числе криминальных структур;

- пропагандистское и психологическое воздействие на политическую ориентацию населения зарубежных и отечественных средств массовой информации в интересах отдельных политических сил;

- отсутствие или несовершенство законодательства, обязывающего органы государственной власти и управления регулярно и полно информировать население о своей деятельности и состоянии дел в сфере своей компетентности;

- препятствия со стороны государства осуществлению законных и равных прав различных политических сил, в том числе оппозиционных, на использование средств массовой информации, контролируемых государством;

- политизация системы формирования общественного мнения, ведущая к искажению реальных ситуаций (фальсификация или предвзятая интерпретация результатов опросов или референдумов).

Основными мероприятиями обеспечения информационной безопасности в политической сфере являются:

- разработка и постоянное совершенствование законодательства, правовых и организационных механизмов, регулирующих взаимоотношения всех субъектов политической жизни в реализации их конституционных прав и обязанностей в использовании средств массовой информации;

- создание системы независимого и гласного контроля за деятельностью государственных средств массовой информации, институтов, центров и служб изучения общественного мнения, а также специальных служб по связи с населением;

- активизация контрпропагандистской деятельности и дипломатических усилий по предотвращению информационно-пропагандистского вмешательства во внутренние дела страны.

В сфере экономики

Среди объектов сферы экономики наиболее подвержены воздействию угроз информационной безопасности: система государственной статистики;

- источники, порождающие информацию о коммерческой деятельности хозяйственных субъектов всех форм собственности, о потребительских свойствах товаров и услуг;

- системы сбора и обработки финансовой, биржевой, налоговой, таможенной информации, информации о внешнеэкономической деятельности государства и коммерческих структур.

Система государственной статистической отчетности должна обладать достаточной защищенностью от серьезных и массовых искажений. Особое

внимание должно уделяться защите первичных источников информации и обобщённых отчетных данных.

В конечном итоге информация в системе государственной статистики должна обладать полнотой, достоверностью, достаточностью, сопоставимостью и регулярностью - свойствами, необходимыми для принятия рациональных решений на уровнях государства, отрасли, предприятия, для проведения общеэкономического анализа и прогнозирования развития народного хозяйства.

Нормальное функционирование хозяйственных объектов нарушается из-за отсутствия нормативно-правовых положений, определяющих ответственность источников информации о коммерческой деятельности и потребительских свойствах товаров Н услуг за недостоверность и сокрытие сведений (о результатах реальной хозяйственной деятельности, об инвестициях и др.). С другой стороны, существенный экономический ущерб может быть нанесен Государственным и предпринимательским структурам вследствие разглашения информации, содержащей коммерческую тайну.

В системах сбора и обработки финансовой, биржевой, налоговой, таможенной информации наибольшую опасность с точки зрения информационной безопасности представляют хищения и преднамеренное искажение информации, возможность которых связана с преднамеренным или случайным Нарушением технологии работы с информацией, несанкционированным доступом к ней, что обусловлено недостаточными мерами защиты информации. Такая же опасность существует в органах, занятых формированием и распространением информации о внешнеэкономической деятельности (центральный аппарат ведомств, торгпредства, таможни и т.п.).

Серьезную опасность для Нормального функционирования сферы экономики в целом представляют все более изощренные компьютерные преступления (подлоги, хищения и т.д.), связанные с проникновением криминальных элементов в компьютерные системы и сети.

Наряду с широким использованием стандартных методов и средств для сферы экономики приоритетными Направлениями обеспечения информационной безопасности являются:

- разработка и принятие правовых положений, устанавливающих ответственность юридических и физических лиц за несанкционированный доступ и хищение информации, преднамеренное распространение недостоверной информации, разглашение коммерческой тайны, утечку конфиденциальной информации;

- коренная перестройка системы государственной статистической отчетности, направленная на повышение достоверности, полноты, сопоставимости и защищенности информации путем введения строгой юридической ответственности первичных источников информации, организации действенного контроля за их деятельностью и деятельностью служб обработки и анализа статистической информации, ограничения ее

коммерциализации, использования специальных организационных и программно-технических средств защиты информации;

- создание и совершенствование специальных средств Защиты финансовой и коммерческой информации;

- разработка комплекса организационно-технических мероприятий по совершенствованию технологии информационной деятельности и защиты информации в хозяйственных, финансовых, промышленных и других экономических структурах с учетом специфических для сферы экономики требований информационной безопасности;

- совершенствование системы профессионального отбора и подготовки персонала систем сбора, обработки, анализа и распространения экономической информации.

В оборонной сфере

К объектам информационной безопасности, в оборонной сфере, наиболее уязвимым со стороны всего комплекса угроз, относятся:

- информационные ресурсы аппарата Министерства обороны, Генерального штаба, главных штабов видов Вооруженных сил и родов войск, научно-исследовательских учреждений, содержащие сведения и данные об оперативных и стратегических планах подготовки и ведения боевых действий, о составе и дислокации войск, о мобилизационной готовности, тактико-технических характеристиках вооружения и военной техники;

- информационные ресурсы предприятий оборонного комплекса, содержащие сведения и данные об их научно-техническом и производственном потенциалах, об объемах поставок и запасах стратегических видов сырья и материалов, об основных направлениях развития вооружения, военной техники, их боевых возможностях и проводимых в интересах обороны фундаментальных и прикладных НИР;

- системы связи и управления войсками и оружием, их информационное обеспечение;

- политико-моральное состояние войск в части, зависящей от информационно-пропагандистского воздействия;

- информационная инфраструктура, в том числе центры обработки и анализа информации Генерального штаба и информационные подразделения штабов видов Вооруженных Сил, штабов объединений и соединений видов Вооруженных Сил и родов войск, пункты управления, узлы и линии радио-, радиорелейной, тропосферной и спутниковой связи, а также линии проводной связи, развертываемые и арендуемые Министерством обороны и другими силовыми структурами.

Из внешних источников угроз в наибольшей степени способны воздействовать на информационную безопасность объектов оборонной сферы следующие:

- все виды разведывательной деятельности зарубежных государств;

- информационно-технические воздействия (методы радиоэлектронной борьбы, проникновение в компьютерные сети и т.п.) со стороны вероятных противников;

- психологические операции вероятных противников, осуществляемые специальными методами и через деятельность средств массовой информации;

- деятельность иностранных политических и экономических структур, направленная против интересов Российской Федерации в оборонной сфере.

Из внутренних источников угроз наибольшую опасность представляют:

- нарушение- установленных регламентов сбора, обработки и передачи информации в штабах и учреждениях Министерства обороны, в организациях и на предприятиях оборонного комплекса;

- преднамеренные действия и непреднамеренные ошибки персонала информационных систем специального назначения;

- отказы технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах специального назначения;

- информационно-пропагандистская деятельность организаций и отдельных лиц, направленная против интересов государства, подрывающая престиж вооруженных сил и их боеготовность.

Эти источники угроз представляют особую опасность в условиях обострения военно-политической обстановки.

Главными направлениями совершенствования информационной безопасности в оборонной сфере являются:

- концептуальное, включающее структуризацию целей обеспечения информационной безопасности в оборонной сфере, вытекающих из них практических задач, корректное определение информационных угроз и их источников;

- техническое, характеризуемое постоянным совершенствованием средств защиты информационных ресурсов от методов и средств несанкционированного доступа к ним, развитием защищенных, засекреченных систем связи и управления войсками и оружием, повышение надежности специального программного обеспечения;

- организационное, связанное с необходимостью формирования оптимальной структуры и состава функциональных органов системы информационной безопасности в оборонной сфере и координации их аффективного взаимодействия, совершенствование приемов и способов стратегической и оперативной маскировки, разведки и радиоэлектронной борьбы, методов и средств активного противодействия информационно-пропагандистским и психологическим операциям вероятного противника.

Кроме того, одним из главных направлений совершенствования информационной безопасности в оборонной сфере является повышение эффективности защиты технологий производства и тактико-технических характеристик вооружения и военной техники. 9

В условиях чрезвычайных ситуаций

Наиболее уязвимыми объектами для угроз информационной безопасности в условиях чрезвычайных ситуаций (ЧС) являются система принятия решений по оперативным действиям (реакциям) на их развитие и ход ликвидации последствий, а также система сбора и обработки информации о возможном возникновении ЧС.

Особое значение для нормального функционирования этих объектов имеет разрушение информационной инфраструктуры (центров сбора и анализа информации, технических средств обработки и передачи информации, систем телекоммуникации и каналов связи) вследствие аварий, катастроф и стихийных бедствий. Эти события, а также задержка, искажение и разрушение оперативной информации, несанкционированный доступ к ней отдельных лиц или групп людей могут привести к тяжелым последствиям.

Особенностью информационного воздействия в условиях ЧС является приведение в движение больших масс людей, испытывающих психический стресс, быстрое распространение панических слухов, ложной или недостоверной информации. Нередко в условиях ЧС имеет место сокрытие информации, приводящее к сложностям при ликвидации ее последствий.

К специфическим для данной сферы направлениям обеспечения информационной безопасности относятся:

- разработка эффективной системы мониторинга признаков — предвестников ЧС;
- повышение надежности средств обработки и передачи информации, обеспечивающих деятельность центров принятия решений по ЧС;
- анализ поведения больших масс людей под воздействием ложной или недостоверной информации и выработка мер по управлению ими в условиях ЧС;
- разработка специальных мер повышения информированности населения в условиях ЧС.

В общегосударственных информационных и телекоммуникационных системах

Основными объектами информационной безопасности в общегосударственных информационных и телекоммуникационных системах являются:

- информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, и конфиденциальную информацию, представленные в виде документированных информационных массивов и баз данных;
- средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, технические средства приема, передачи и обработки информации (звукозаписи, звукоусиления, звукосопровождения, переговорные и

телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки графической, смысловой и буквенно-цифровой информации), используемые для обработки информации ограниченного доступа, их информативные физические поля;

- технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается (циркулирует) информация, содержащая сведения, отнесенные к государственной или служебной тайне, а также сами помещения, предназначенные для секретных переговоров.

Основными источниками угроз в сфере информационной безопасности являются деятельность иностранных разведывательных и специальных служб, преступных групп и формирований, противозаконная деятельность отдельных лиц, нарушение установленных регламентов сбора, обработки и передачи информации, преднамеренные действия и непреднамеренные ошибки персонала информационных систем, отказы технических средств и сбои программного обеспечения в информационных и телекомуникационных системах.

Основными направлениями обеспечения информационной безопасности в общегосударственных информационных и телекоммуникационных системах являются:

- предотвращение перехвата с помощью технических средств информации, передаваемой по каналам связи;
- исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации;
- предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, создаваемых функционирующими техническими средствами, а также электроакустических преобразовании;
- предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации;
- выявление внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств);
- предотвращение перехвата техническими средствами речевой информации из помещений и объектов.

Предотвращение перехвата с помощью технических средств информации, передаваемой по каналам связи, достигается применением криптографических и иных методов и средств защиты, а также проведением организационно-технических и режимных мероприятий.

Исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации достигается применением специальных программно-технических средств защиты, использованием криптографических способов защиты, а также организационными и режимными мероприятиями.

Предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, а также электроакустических преобразований достигается применением защищенных технических средств, аппаратных средств защиты, средств активного противодействия, экранированием зданий или отдельных помещений, установлением контролируемой зоны вокруг средств информатизации и другими организационными и техническими мерами.

Предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации, достигается применением специальных программных и аппаратных средств защиты (антивирусные процессоры, антивирусные программы), организацией системы контроля безопасного программного обеспечения.

Выявление внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств) достигается проведением специальных проверок.

Предотвращение перехвата техническими средствами речевой информации из помещений и объектов достигается применением специальных средств защиты, проектными решениями, обеспечивающими звукоизоляцию помещений, выявлением специальных устройств подслушивания и другими организационными и режимными мероприятиями.

Основными организационно-техническими мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:

- лицензирование деятельности предприятий в области защиты информации;
- аттестация объектов информатизации по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности;
- сертификация средств защиты информации и контроля за ее эффективностью, систем и средств информатизации и связи в части защищенности информации от утечки по техническим каналам;
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;
- создание и применение информационных и автоматизированных систем управления в защищенном исполнении;
- разработка и использование средств защиты информации и методов контроля за ее эффективностью;
- применение специальных методов, технических мер и средств защиты, исключающих перехват информации, передаваемой по каналам связи.

Конкретные методы, приемы и меры защиты информации разрабатываются в зависимости от степени возможного ущерба в случаях ее утечки, разрушения или уничтожения.

В области науки и техники

Наиболее уязвимыми объектами информационной безопасности в области науки и техники являются:

- результаты фундаментальных, поисковых и прикладных научных исследований, содержащие сведения, данные и знания, потенциально важные для научно-технического, технологического и социально-экономического развития страны, утрата которых может нанести ущерб национальным интересам и престижу Российской Федерации;

- незапатентованные технологии, ноу-хау, промышленные образцы, модели и экспериментальное оборудование, для которых еще не определен статус конфиденциальности и которые поэтому не подпадают под действующее законодательство и могут быть проданы или переданы за рубеж;

- объекты интеллектуальной собственности (открытия, патенты, изобретения, промышленные образцы, программные продукты и пр.), которые могут быть похищены и незаконно распространены или использованы, несмотря на их правовую защиту.

Специфика угроз перечисленным объектам информационной безопасности состоит в их многообразии, сложности идентификации, поскольку, как правило, они носят уникальный или индивидуальный характер» При классификации угроз в этой области необходимо уделять особое внимание изучению возможности промышленного шпионажа специальных служб и криминальных структур.

Вследствие этой специфики объекты информационной безопасности в области науки, техники и технологии трудно защитимы. Должна быть организована система оценки возможных последствий воздействия угроз на указанные объекты, включающая общественные научные советы и институт независимых экспертиз, вырабатывающие рекомендации для каждого конкретного случая распространения или использования научной, технической и технологической продукции с целью предотвращения незаконного присвоения или Использования научного и интеллектуального потенциала.

Реальный путь противодействия угрозам со стороны государства заключается в постоянном совершенствовании законодательства в этой области и механизмов его реализации. Многие мероприятия по предотвращению или нейтрализации угроз в этой области, особенно в части, касающейся научных кадров, лежат в сфере социальной и экономической политики государства.

В сфере духовной жизни и информационной безопасности личности

Объектами информационной безопасности в духовной сфере являются мировоззрение людей, их жизненные ценности и идеалы, социальные и личностные ориентации, их культурные и эстетические позиции. Оценка последствий тех или иных информационных воздействий в этой сфере весьма затруднительна и должна производиться с учетом конкретно складывающейся обстановки.

Сфера духовной жизни весьма чувствительна к информационно-пропагандистскому воздействию, идеологическому давлению, культурной экспансии, которые осуществляются, главным образом, через средства массовой информации и могут рассматриваться как информационные угрозы духовному здоровью населения страны. Средства массовой информации играют определяющую роль в формировании духовной жизни. В этом состоит их особая ответственность перед обществом.

Сами информационные воздействия осуществляются в гибких, постоянно изменяющихся формах, что обусловливает сложность определения их влияния на различные составляющие духовной сферы. Это особенно характерно для современного периода развития России, когда по существу не сформулированы национальные приоритеты и идеология перестраивающихся общества и государства.

Предотвращение и нейтрализация угроз информационной безопасности в сфере духовной жизни требуют, прежде всего, открытого провозглашения государственной, официальной идеологии, приемлемой для большинства населения и учитывающей культурные и исторические традиции многонациональной страны. Лишь на основе такой идеологии могут быть выработаны четкие критерии оценки угроз информационной безопасности, основные приоритеты и государственная политика в этой сфере.

Главным представляется разработка и осуществление цивилизованных, демократических форм и методов воздействия на средства массовой информации в целях формирования и распространения духовных ценностей, отвечающих национальным интересам страны, воспитания гражданского и патриотического долга и защиты от враждебной или недружественной пропаганды.

Необходимо также разработать специальные правовые и организационные мероприятия, препятствующие коммерциализации культуры и обеспечивающие сохранение и развитие информационных ресурсов, составляющих большую культурно-историческую ценность.

Основным носителем духовных ценностей является личность, постоянно испытывающая информационные воздействия, направленные на формирование ее отношения к действительности, идеалов и устремлений, мотиваций и уровня притязаний. Эти воздействия могут создавать эмоциональный дискомфорт, вызывать стрессы и нарушать физическую, социальную или духовную целостность личности.

Обеспечение информационной безопасности личности означает ее право на получение объективной информации и предполагает, что полученная человеком из разных источников информация не препятствует свободному формированию и развитию его личности. В качестве воздействия на личность может выступать:

- целенаправленное информационное давление с целью изменения мировоззрения, политических взглядов и морально-психологического состояния людей;

- распространение недостоверной, искаженной, неполной информации; использование неадекватного восприятия людьми достоверной информации.

Особую роль в воздействии на сознание и поведение отдельной личности играют средства массовой информации, которые в силу своей общедоступности и распространенности оказывают непосредственное влияние на мировоззренческие установки, субъективные ценности и предпочтения, регуляцию поступков и взаимодействие с другими людьми.

При организации противодействия угрозам информационной безопасности личности необходимо учитывать индивидуальные и личностные особенности людей, сформированные предыдущим опытом, мотивами и интересами, интеллектуальным уровнем, социально-демографическими характеристиками, социальным статусом, стереотипами и другими факторами.

Выбор адекватных способов воздействия (убеждения, внушения, разъяснения), адекватных средств (аудио, визуальных, электронных, печатных) зависят от полноты учета всех характеристик личности и ситуации. Одним из важнейших способов противодействия является упреждающее информационное воздействие.

Устойчивость к воздействиям извне определяется личностными качествами человека, которые во многом определяются постоянными информационными воздействиями, главным образом со стороны средств массовой информации. Они несут основную ответственность за формирование личностных и гражданских качеств, способных противостоять информационным угрозам. Особенно это важно в настоящее время, когда в обществе проявляются низкий уровень правосознания, непонимание людьми ценности информации.

Информационные угрозы, вызывающие сознательные или непреднамеренные нарушения информационной безопасности лиц, работающих в информационных системах и средствах массовой информации, должны парироваться посредством разъяснения их прав, регламентации обязанностей и разделения ответственности, обучения и тренинга персонала, а в особо важных случаях — путем отбора специалистов по психологическим критериям.

V. ОСНОВЫ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

5.1. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации

Государственная политика обеспечения информационной безопасности в Российской Федерации (далее — Государственная политика) формирует направления деятельности органов государственной власти и управления в области обеспечения информационной безопасности, включая гарантии прав всех субъектов на информацию, закрепление обязанностей и ответственности государства и его органов за информационную безопасность страны, и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

Государственная политика является открытой и предусматривает информированность общества о деятельности государственных органов и общественных институтов в области информационной безопасности с учетом ограничений, предусмотренных действующим законодательством.

Государственная политика исходит из принципа безусловного правового равенства всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса. Она основывается на обязательном обеспечении прав граждан и организаций на свободное создание, поиск, получение и распространение информации любым законным способом, В этих целях государство совершенствует существующее и разрабатывает новое законодательство и нормативно-правовую базу информационных отношений в обществе, а также осуществляет контроль за безусловным их исполнением.

Государство исходит из того, что информационные ресурсы являются объектом собственности, способствует введению их в хозяйственный оборот при соблюдении законных интересов собственников, владельцев и распорядителей информационных ресурсов.

Государство считает приоритетным развитие современных информационных и телекоммуникационных технологий и технических средств, способных обеспечить создание национальных телекоммуникационных сетей и включение России в глобальные информационные сети и системы мониторинга.

Исходя из принципа разделения ответственности между органами федеральной, региональной власти и местного самоуправления, государственная политика предусматривает согласованность организационных и технических решений, принимаемых этими органами для обеспечения информационной безопасности в рамках единого информационного пространства России.

Государственная политика не допускает монополизма министерств, ведомств и организаций в области обеспечения информационной безопасности.

Государственная политика обеспечения информационной безопасности исходит из следующих основных положений:

- ограничение доступа к информации есть исключение из общего принципа открытости информации и осуществляется только на основе законодательства;

- ответственность за сохранность информации, ее засекречивание и рассекречивание персонифицируется;

- доступ к какой-либо информации, а также вводимые ограничения доступа осуществляются с учетом определяемых законом прав собственности на эту информацию;

- государство формирует нормативно-правовую базу, регламентирующую права, обязанности и ответственность всех субъектов, действующих в информационной сфере;

- юридические и физические лица, собирающие, накапливающие и обрабатывающее персональные данные и конфиденциальную информацию, несут ответственность перед законом за их сохранность и использование;

- государство законными средствами обеспечивает защиту общества от ложной, искаженной и недостоверной информации, поступающей через средства массовой информации;

- государство осуществляет контроль за созданием и использованием средств защиты информации посредством их обязательной сертификации и лицензирования деятельности в области защиты информации;

- государство проводит протекционистскую политику, поддерживающую деятельность отечественных производителей средств информатизации и защиты информации и осуществляет меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;

- государство способствует предоставлению гражданам доступа к мировым информационным ресурсам, глобальным информационным сетям;

- государство стремится к отказу от зарубежных информационных технологий для информатизации органов государственной власти и управления по мере создания конкурентоспособных отечественных информационных технологий и средств информатизации;

- государство формирует Федеральную программу информационной безопасности, объединяющую усилия государственных организаций и коммерческих структур в создании единой системы информационной безопасности России;

- государство прилагает усилия для противодействия информационной экспансии США и других развитых стран, поддерживает интернационализацию глобальных информационных сетей и систем.

На основе изложенных принципов и положений определяются общие направления формирования и реализации политики информационной безопасности в политической, военной, экономической и других сферах деятельности государства.

Государственная политика в качестве механизма Согласования интересов субъектов информационных отношений и нахождения компромиссных решений предусматривает формирование и организацию эффективной работы различных советов, комитетов и комиссий с широким представительством специалистов, и всех заинтересованных структур.

Механизмы реализации Государственной политики должны быть гибкими и своевременно отражать изменения, происходящие в политической и экономической жизни страны.

5.2. Основные положения государственной политики обеспечения информационной безопасности субъектов Российской Федерации

Конституционные основы федеративного государственного устройства страны нуждаются в развитии и распространении на все сферы жизнедеятельности личности, общества и государства, включая сферу обеспечения информационной безопасности.

Информационная безопасность должна быть предметом ответственности органов государственной власти и управления всех уровней с учетом закрепленного в Конституции Российской Федерации разграничения предметов ведения и полномочии между ними.

Разработка региональных вопросов обеспечения информационной безопасности имеет ряд особенностей, объективно связанных с федеративным устройством страны.

Информационная собственность субъектов Российской Федерации является разновидностью государственной собственности субъектов Российской Федерации.

Она включает в себя:

- информационную собственность органов власти и управления субъектов Российской Федерации;
- информационную собственность предприятий и учреждений, созданных или приобретенных за счет средств субъектов Российской Федерации;
- культурные ценности народов, населяющих территорию субъектов Российской Федерации.

Обязанностью органов власти и управления субъектов Российской Федерации является защита права информационной собственности, находящейся на территории субъектов Российской Федерации объектов федеральной информационной собственности, информационной собственности органов местного, самоуправления, других юридических и физических лиц.

Субъекты Российской Федерации обладают всей полнотой информационных прав, действующих в Российской Федерации. Эти права от имени субъектов Российской Федерации осуществляют их органы государственной власти и управления.

Субъектам Российской Федерации гарантируется:

- равное право доступа на российский рынок информации и средств обеспечения информационной безопасности, находящихся в любой форме собственности;

- право использования для решения региональных государственных задач федеральных информационных банков данных с соблюдением установленных правил обеспечения информационной безопасности;

- право проведения самостоятельной внутренней и внешнеэкономической деятельности в сфере информационной безопасности в рамках, определенных федеральными законами;

- право осуществлять защиту своих информационных прав и права информационной собственности как самостоятельно, так и путем обращения в федеральные и международные правозащитные органы.

Более подробная проработка основных направлений региональной политики обеспечения информационной безопасности должна быть осуществлена субъектами Российской федерации с учетом особенностей их территорий, состояния и перспектив развития хозяйственной сферы.

5.3. Правовое обеспечение информационной безопасности Российской Федерации

Правовое обеспечение рассматривается как приоритетное направление формирования механизмов реализации политики обеспечения информационной безопасности в Российской Федерации.

Правовое обеспечение включает в себя:

- нормотворческую деятельность по созданию законодательства, регулирующего отношения в обществе, связанные с обеспечением информационной безопасности;

- исполнительную и правоприменительную деятельность по исполнению законодательства в области информации, информатизации и защиты информации органами государственной власти и управления, организациями (юридическими лицами), гражданами.

Нормотворческая деятельность в области обеспечения информационной безопасности предусматривает:

- оценку состояния действующего законодательства и разработку программы его совершенствования;

- создание организационно-правовых механизмов обеспечения информационной безопасности;

- формирование правового статуса всех субъектов в системе информационной безопасности, пользователей информационных и телекоммуникационных систем и определение их ответственности за обеспечение информационной безопасности;

- разработку организационно-правового механизма сбора и анализа статистических данных о воздействии угроз информационной безопасности и их последствиях с учетом всех видов (категорий) информации;

- разработку законодательных и других нормативных актов, регулирующих порядок ликвидации последствий воздействий угроз,

восстановления нарушенного права и ресурсов, реализации компенсационных мер.

Исполнительная и правоприменительная деятельность предусматривает разработку процедур применения законодательства и нормативных актов к субъектам, совершившим преступления и проступки при работе с закрытой информацией и* нарушившим регламент информационных взаимодействий, а также правонарушения с использованием незащищенных средств информатизации, разработку составов правонарушений с учетом специфики уголовной, гражданской, административной, дисциплинарной ответственности.

Вся деятельность по правовому обеспечению информационной безопасности должна строиться на основе трех фундаментальных положений права — соблюдение законности, обеспечение баланса интересов отдельных субъектов и государства, неотвратимость наказания.

Соблюдение законности предполагает наличие законов и иных нормативных установлений, их применение и исполнение субъектами права в области информационной безопасности.

Обеспечение баланса интересов граждан, других субъектов информационных отношений и государства предусматривает приоритет государственных интересов как общих интересов всех субъектов. Ориентация на свободы, права и интересы граждан не принижает роль государства в обеспечении национальной безопасности в целом и в области информационной безопасности в частности.

Неотвратимость наказания предусматривает соответствующую степень ответственности в области обеспечения информационной безопасности, которая реализуется с учетом повышенной социальной опасности угроз информационной среде общества.

Реализация механизмов правового обеспечения информационной безопасности должна опираться на информатизацию правовой сферы в целом.

5.4. Первоочередные мероприятия по реализации государственной политики информационной безопасности Российской Федерации

Первоочередные мероприятия по реализации государственной политики информационной безопасности Российской Федерации должны включать:

- разработку форм, методов и средств реализации государственной политики, подготовку решений органов исполнительной власти и документов, закрепляющих ее основные положения;

- создание нормативно-правовой базы реализации государственной политики в области информационной безопасности, в том числе определение последовательности и порядка разработки законодательных и нормативно-правовых актов, а также механизмов практической реализации принятого законодательства;

- анализ технико-экономических параметров отечественных и зарубежных программно-технических средств обеспечения информационной безопасности и выбор перспективных направлений развития отечественной техники;

- формирование Государственной научно-технической программы совершенствования и развития методов и средств обеспечения информационной безопасности, предусматривающей их использование в национальных информационных и телекоммуникационных сетях и системах с учетом перспективы вхождения России в глобальные информационные сети и системы;

- создание системы сертификации на соответствие требованиям информационной безопасности отечественных и закупаемых импортных средств информатизации, используемых в государственных органах власти и управления;

- совершенствование организационной структуры системы информационной безопасности Российской. Федерации, предусматривающее создание единого центра координации и регулирования деятельности всех органов, входящих в систему;

- разработка системы экономических и статистических показателей, характеризующих эффективность функционирования системы обеспечения информационной безопасности;

- определение реальных потребностей системы информационной безопасности в специалистах, организация системы отбора, подготовки и переподготовки кадров.

VI. ОРГАНИЗАЦИОННАЯ СТРУКТУРА И ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

6.1. Организационная структура системы информационной безопасности Российской Федерации

Анализ состояния информационной безопасности в стране диктует необходимость реформирования существующей организации обеспечения информационной безопасности с целью создания целостной, системы обеспечения информационной безопасности Российской Федерации (далее — Система).

Система является составной частью общей системы национальной безопасности страны, представляет собой совокупность органов государственной власти и управления и предприятий, согласованно осуществляющих, деятельность по обеспечению' информационной безопасности на основе единых правовых норм.

Организационную структуру Системы составляют:

- органы государственной власти и управления Российской Федерации и субъектов Российской Федерации, решающие задачи обеспечения информационной безопасности в пределах своей компетенции;

- государственные и межведомственные комиссии и советы, специализирующиеся на проблемах информационной безопасности;

- структурные и межотраслевые подразделения по защите информации органов государственной власти и управления, а также структурные подразделения предприятий, проводящие работы с использованием сведений, отнесенных к государственной тайне, или специализирующиеся на проведении работ в области защиты информации;

- научно-исследовательские, проектные и конструкторские организации, выполняющие работы по обеспечению информационной безопасности;

- учебные заведения, осуществляющие подготовку и переподготовку кадров для работы в системе обеспечения информационной безопасности.

Особое место в системе информационной безопасности занимают государственные и общественные организации, осуществляющие законный контроль за деятельностью государственных и негосударственных средств массовой информации.

6.2. Основные функции системы информационной безопасности Российской Федерации

Система информационной безопасности осуществляет свою деятельность на основе государственной политики обеспечения национальной безопасности Российской Федерации.

Основными функциями системы обеспечения информационной безопасности Российской Федерации являются:

- разработка и реализация стратегии обеспечения информационной безопасности;

- реализация прав граждан и организаций на получение, распространение и использование информации;

- оценка состояния информационной безопасности в стране, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, парирования и нейтрализации этих угроз;

- координация и контроль деятельности субъектов системы информационной безопасности;

- организация разработки федеральных и ведомственных программ обеспечения информационной безопасности и координация работ по их реализации;

- проведение единой технической политики в области обеспечения информационной безопасности;

- организация фундаментальных, поисковых и прикладных научных исследований в области информационной безопасности;

- обеспечение контроля за созданием и использованием средств защиты информации посредством обязательного лицензирования деятельности в области защиты информации и сертификации средств защиты информации;

- осуществление международного сотрудничества в сфере информационной безопасности, представление интересов Российской Федерации в соответствующих международных организациях.

Система должна обеспечивать гибкое управление процессами информационной безопасности на государственном, региональном, отраслевом, производственном и пользовательском уровнях.

Масштабность, сложность и разнообразие перечисленных функций требуют создания иерархической организационной структуры, обеспечивающей координацию деятельности всех составляющих системы информационной безопасности.

Построение Системы осуществляется на основе разграничения предметов ведения и полномочий федеральных и региональных органов государственной власти, с учетом согласованности деятельности территориальных органов федеральной исполнительной власти и органов власти субъектов Российской Федерации.

VII. МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО ПО ВОПРОСАМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Международное сотрудничество в области информационной безопасности (далее — сотрудничество) есть неотъемлемая составляющая политического, военного, экономического, культурного й других видов взаимодействия стран — участников мирового сообщества.

Сотрудничество должно способствовать повышению информационной безопасности всех членов мирового сообщества, включая Российскую Федерацию.

Основными направлениями сотрудничества, отвечающими интересам Российской Федерации, являются:

- предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских сетях и в каналах информационного обеспечения мировой торговли, к конфиденциальной информации в международных политических, экономических и военных союзах, блоках и организациях, к информации в международных правоохранительных организациях, ведущих борьбу с международной организованной преступностью, международным терроризмом, распространением наркотиков и незаконной торговлей оружием и расщепляющимися материалами;

- обеспечение информационной безопасности трансграничного информационного обмена и его информационного регламента, а также сохранности и неискаженности информации при ее передаче по национальным телекоммуникационным каналам и каналам связи;

- координация деятельности государств — участников международного сотрудничества по предотвращению компьютерных преступлений.

Особое внимание в ходе сотрудничества должно быть уделено проблемам взаимодействия со странами СНГ с учетом перспектив создания единого информационного пространства на территории бывшего СССР, в

пределах которого используются практически единые телекоммуникационные системы и линии связи.

Для реализации указанных направлений сотрудничества необходимо:

- активное участие России во всех международных организациях, действующих в области информационной безопасности;
- обмен опытом в области обеспечения информационной безопасности, в том числе через международные и отечественные печатные издания;
- расширение участия российских специалистов в международных конференциях, семинарах, выставках.

Для разработки методологических и научно-технических проблем обеспечения международной информационной безопасности целесообразно создание под эгидой ООН Международного научно-исследовательского института.

5. ИНФОРМАЦИОННАЯ ВОЙНА, МЕТОДЫ И СРЕДСТВА ЕЁ ВЕДЕНИЯ

Информационная война воздействует на сознание масс людей и является частью борьбы между различными цивилизационными системами. Она проводится в информационном пространстве при помощи специально предназначенных для этого средств управления информационными ресурсами и при помощи информационного оружия

Методы и инструменты информационной войны.

- социальный контроль, то есть влияние на широкие слои общества;
- социальное манипулирование, то есть целенаправленное воздействие на общество с целью достижения определенных целей;
- манипулирование информацией, то есть использование правдивой информации таким образом, чтобы из нее были сделаны неверные выводы;
- дезинформация, то есть распространение искаженной или сфабрикованной информации (или и того и другого одновременно);
- фабрикация информации, то есть создание заведомо ложной информации.
- лоббирование,
- шантаж,
- вымогательство,
- информационный терроризм.

Средствами ведения информационной войны могут быть:

- компьютерные вирусы, отличающиеся высокой способностью проникновения по различным каналам в программы, закрепления и размножения в них, подавления и вывода их из строя;
- «логические бомбы», «программы-оборотни», «программы-убийцы информации» заранее внедряемые в информационно-управляющие центры военной и гражданской инфраструктуры, и по сигналу или в установленное время искажающие, уничтожающие информацию или дезорганизующие работу программно-технических средств;
- программы несанкционированного доступа к информационным ресурсам противника с целью хищения разведывательной информации;
- средства подавления информационных систем противника, вхождения в них в целях подмены информации или открытого пропагандистского вмешательства;
- биотехнологические средства, созданные на основе клеточной инженерии, выводящие из строя компьютерные платы;
- средства внедрения вирусов, логических бомб, программ оборотней, программ-убийц информации, программ воздействия на персонал («зомбирование») и др. в информационные системы (вирусные пушки, закладки в микропроцессоры, международные компьютерные сети и др.);

Основной прием информационной войны - это манипулирование близкой для определенной социальной группы идеологией посредством ее радикализации.

6. ПРОГРАММА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИИ И ПУТИ ЕЕ РЕАЛИЗАЦИИ

Важнейшим документом в сфере информационной политики, который был принят в России и реализуется в настоящее время, является Доктрина информационной безопасности.

I. Общие положения

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

В настоящей Доктрине под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет»), сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

2. В настоящей Доктрине используются следующие основные понятия:

а) национальные интересы Российской Федерации в информационной сфере (далее - национальные интересы в информационной сфере) - объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы;

б) угроза информационной безопасности Российской Федерации (далее - информационная угроза) - совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере;

в) информационная безопасность Российской Федерации (далее - информационная безопасность) - 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;

г) обеспечение информационной безопасности - осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

д) силы обеспечения информационной безопасности - государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности;

е) средства обеспечения информационной безопасности - правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности;

ж) система обеспечения информационной безопасности - совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности;

з) информационная инфраструктура Российской Федерации (далее - информационная инфраструктура) - совокупность объектов информатизации, информационных систем, сайтов в сети «Интернет» и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации.

3. В настоящей Доктрине на основе анализа основных информационных угроз и оценки состояния информационной безопасности определены стратегические цели и основные направления обеспечения информационной безопасности с учетом стратегических национальных приоритетов Российской Федерации.

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

5. Настоящая Доктрина 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 2015 г. № 683, а также других документов стратегического планирования в указанной сфере.

6. Настоящая Доктрина является основой для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также для выработки мер по совершенствованию системы обеспечения информационной безопасности.

II. Национальные интересы в информационной сфере

7. Информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства. Их эффективное

применение является фактором ускорения экономического развития государства и формирования информационного общества.

Информационная сфера играет важную роль в обеспечении реализации стратегических национальных приоритетов Российской Федерации.

8. Национальными интересами в информационной сфере являются:

а) обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, обеспечение информационной поддержки демократических институтов, механизмов взаимодействия государства и гражданского общества, а также применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации;

б) обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура) и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы агрессии и в военное время;

в) развитие в Российской Федерации отрасли информационных технологий и электронной промышленности, а также совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности;

г) доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации и ее официальной позиции по социально значимым событиям в стране и мире, применение информационных технологий в целях обеспечения национальной безопасности Российской Федерации в области культуры;

д) содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также на защиту суверенитета Российской Федерации в информационном пространстве.

9. Реализация национальных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры в целях обеспечения конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также национальной безопасности Российской Федерации.

III. Основные информационные угрозы и состояние информационной безопасности

10. Расширение областей применения информационных технологий, являясь фактором развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые информационные угрозы.

Возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности.

При этом практика внедрения информационных технологий без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз.

11. 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.

Одновременно с этим усиливается деятельность организаций, осуществляющих техническую разведку в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса.

12. Расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств. В эту деятельность вовлекаются религиозные, этнические, правозащитные и иные организации, а также отдельные группы граждан, при этом широко используются возможности информационных технологий.

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.

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

13. Различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии,

а также привлечения к террористической деятельности новых сторонников. Такими организациями в противоправных целях активно создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры.

14. Возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее.

15. Состояние информационной безопасности в области обороны страны характеризуется увеличением масштабов применения отдельными государствами и организациями информационных технологий в военно-политических целях, в том числе для осуществления действий, противоречащих международному праву, направленных на подрыв суверенитета, политической и социальной стабильности, территориальной целостности Российской Федерации и ее союзников и представляющих угрозу международному миру, глобальной и региональной безопасности.

16. Состояние информационной безопасности в области государственной и общественной безопасности характеризуется постоянным повышением сложности, увеличением масштабов и ростом скоординированности компьютерных атак на объекты критической информационной инфраструктуры, усилением разведывательной деятельности иностранных государств в отношении Российской Федерации, а также нарастанием угроз применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности Российской Федерации.

17. Состояние информационной безопасности в экономической сфере характеризуется недостаточным уровнем развития конкурентоспособных информационных технологий и их использования для производства продукции и оказания услуг. Остается высоким уровень зависимости отечественной промышленности от зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи, что обусловливает зависимость социально-экономического развития Российской Федерации от геополитических интересов зарубежных стран.

18. Состояние информационной безопасности в области науки, технологий и образования характеризуется недостаточной эффективностью научных исследований, направленных на создание перспективных информационных технологий, низким уровнем внедрения отечественных разработок и недостаточным кадровым обеспечением в области информационной безопасности, а также низкой осведомленностью граждан в вопросах обеспечения личной информационной безопасности. При этом

мероприятия по обеспечению безопасности информационной инфраструктуры, включая ее целостность, доступность и устойчивое функционирование, с использованием отечественных информационных технологий и отечественной продукции зачастую не имеют комплексной основы.

19. Состояние информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства характеризуется стремлением отдельных государств использовать технологическое превосходство для доминирования в информационном пространстве.

Существующее в настоящее время распределение между странами ресурсов, необходимых для обеспечения безопасного и устойчивого функционирования сети «Интернет», не позволяет реализовать совместное справедливое, основанное на принципах доверия управление ими.

Отсутствие международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения, учитывающих специфику информационных технологий, затрудняет формирование системы международной информационной безопасности, направленной на достижение стратегической стабильности и равноправного стратегического партнерства.

IV. Стратегические цели и основные направления обеспечения информационной безопасности

20. 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.

21. В соответствии с военной политикой Российской Федерации основными направлениями обеспечения информационной безопасности в области обороны страны являются:

а) стратегическое сдерживание и предотвращение военных конфликтов, которые могут возникнуть в результате применения информационных технологий;

б) совершенствование системы обеспечения информационной безопасности Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, включающей в себя силы и средства информационного противоборства;

в) прогнозирование, обнаружение и оценка информационных угроз, включая угрозы Вооруженным Силам Российской Федерации в информационной сфере;

г) содействие обеспечению защиты интересов союзников Российской Федерации в информационной сфере;

д) нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества.

22. Стратегическими целями обеспечения информационной безопасности в области государственной и общественной безопасности являются защита суверенитета, поддержание политической и социальной стабильности, территориальной целостности Российской Федерации, обеспечение основных прав и свобод человека и гражданина, а также защита критической информационной инфраструктуры.

23. Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются:

а) противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации;

б) пресечение деятельности, наносящей ущерб национальной безопасности Российской Федерации, осуществляемой с использованием технических средств и информационных технологий специальными службами и организациями иностранных государств, а также отдельными лицами;

в) повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры;

г) повышение безопасности функционирования объектов информационной инфраструктуры, в том числе в целях обеспечения устойчивого взаимодействия государственных органов, недопущения иностранного контроля за функционированием таких объектов, обеспечение целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации, а также обеспечение безопасности информации, передаваемой по ней и обрабатываемой в информационных системах на территории Российской Федерации;

д) повышение безопасности функционирования образцов вооружения, военной и специальной техники и автоматизированных систем управления;

е) повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям;

ж) обеспечение защиты информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа и распространения, в том числе за счет повышения защищенности соответствующих информационных технологий;

з) совершенствование методов и способов производства и безопасного применения продукции, оказания услуг на основе информационных технологий с использованием отечественных разработок, удовлетворяющих требованиям информационной безопасности;

и) повышение эффективности информационного обеспечения реализации государственной политики Российской Федерации;

к) нейтрализация информационного воздействия, направленного на размывание традиционных российских духовно-нравственных ценностей.

24. Стратегическими целями обеспечения информационной безопасности в экономической сфере являются сведение к минимально возможному уровню влияния негативных факторов, обусловленных недостаточным уровнем развития отечественной отрасли информационных технологий и электронной промышленности, разработка и производство конкурентоспособных средств обеспечения информационной безопасности, а также повышение объемов и качества оказания услуг в области обеспечения информационной безопасности.

25. Основными направлениями обеспечения информационной безопасности в экономической сфере являются:

а) инновационное развитие отрасли информационных технологий и электронной промышленности, увеличение доли продукции этой отрасли в валовом внутреннем продукте, в структуре экспорта страны;

б) ликвидация зависимости отечественной промышленности от зарубежных информационных технологий и средств обеспечения информационной безопасности за счет создания, развития и широкого внедрения отечественных разработок, а также производства продукции и оказания услуг на их основе;

в) повышение конкурентоспособности российских компаний, осуществляющих деятельность в отрасли информационных технологий и электронной промышленности, разработку, производство и эксплуатацию средств обеспечения информационной безопасности, оказывающих услуги в области обеспечения информационной безопасности, в том числе за счет создания благоприятных условий для осуществления деятельности на территории Российской Федерации;

г) развитие отечественной конкурентоспособной электронной компонентной базы и технологий производства электронных компонентов, обеспечение потребности внутреннего рынка в такой продукции и выхода этой продукции на мировой рынок.

26. Стратегической целью обеспечения информационной безопасности в области науки, технологий и образования является поддержка инновационного и ускоренного развития системы обеспечения информационной безопасности, отрасли информационных технологий и электронной промышленности.

27. Основными направлениями обеспечения информационной безопасности в области науки, технологий и образования являются:

а) достижение конкурентоспособности российских информационных технологий и развитие научно-технического потенциала в области обеспечения информационной безопасности;

б) создание и внедрение информационных технологий, изначально устойчивых к различным видам воздействия;

в) проведение научных исследований и осуществление опытных разработок в целях создания перспективных информационных технологий и средств обеспечения информационной безопасности;

г) развитие кадрового потенциала в области обеспечения информационной безопасности и применения информационных технологий;

д) обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности.

28. Стратегической целью обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства является формирование устойчивой системы неконфликтных межгосударственных отношений в информационном пространстве.

29. Основными направлениями обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства являются:

а) защита суверенитета Российской Федерации в информационном пространстве посредством осуществления самостоятельной и независимой политики, направленной на реализацию национальных интересов в информационной сфере;

б) участие в формировании системы международной информационной безопасности, обеспечивающей эффективное противодействие использованию информационных технологий в военно-политических целях, противоречащих международному праву, а также в террористических, экстремистских, криминальных и иных противоправных целях;

в) создание международно-правовых механизмов, учитывающих специфику информационных технологий, в целях предотвращения и урегулирования межгосударственных конфликтов в информационном пространстве;

г) продвижение в рамках деятельности международных организаций позиции Российской Федерации, предусматривающей обеспечение равноправного и взаимовыгодного сотрудничества всех заинтересованных сторон в информационной сфере;

д) развитие национальной системы управления российским сегментом сети «Интернет».

V. Организационные основы обеспечения информационной безопасности

30. Система обеспечения информационной безопасности является частью системы обеспечения национальной безопасности Российской Федерации.

Обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

31. Система обеспечения информационной безопасности строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере с учетом предметов ведения федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, а также органов местного самоуправления, определяемых законодательством Российской Федерации в области обеспечения безопасности.

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

33. Организационную основу системы обеспечения информационной безопасности составляют: Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, Центральный банк Российской Федерации, Военно-промышленная комиссия Российской Федерации, межведомственные органы, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационной безопасности.

Участниками системы обеспечения информационной безопасности являются: собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты, средства массовой информации и массовых коммуникаций, организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка, операторы связи, операторы информационных систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, организации, осуществляющие образовательную деятельность в данной

области, общественные объединения, иные организации и граждане, которые в соответствии с законодательством Российской Федерации участвуют в решении задач по обеспечению информационной безопасности.

34. Деятельность государственных органов по обеспечению информационной безопасности основывается на следующих принципах:

а) законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений, основанные на конституционном праве граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом;

б) конструктивное взаимодействие государственных органов, организаций и граждан при решении задач по обеспечению информационной безопасности;

в) соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере;

г) достаточность сил и средств обеспечения информационной безопасности, определяемая в том числе посредством постоянного осуществления мониторинга информационных угроз;

д) соблюдение общепризнанных принципов и норм международного права, международных договоров Российской Федерации, а также законодательства Российской Федерации.

35. Задачами государственных органов в рамках деятельности по обеспечению информационной безопасности являются:

а) обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере;

б) оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;

в) планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности;

г) организация деятельности и координация взаимодействия сил обеспечения информационной безопасности, совершенствование их правового, организационного, оперативно-розыскного, разведывательного, контрразведывательного, научно-технического, информационно-аналитического, кадрового и экономического обеспечения;

д) выработка и реализация мер государственной поддержки организаций, осуществляющих деятельность по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, а также организаций, осуществляющих образовательную деятельность в данной области.

36. Задачами государственных органов в рамках деятельности по развитию и совершенствованию системы обеспечения информационной безопасности являются:

а) укрепление вертикали управления и централизация сил обеспечения информационной безопасности на федеральном, межрегиональном, региональном, муниципальном уровнях, а также на уровне объектов информатизации, операторов информационных систем и сетей связи;

б) совершенствование форм и методов взаимодействия сил обеспечения информационной безопасности в целях повышения их готовности к противодействию информационным угрозам, в том числе путем регулярного проведения тренировок (учений);

в) совершенствование информационно-аналитических и научно-технических аспектов функционирования системы обеспечения информационной безопасности;

г) повышение эффективности взаимодействия государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности.

37. Реализация настоящей Доктрины осуществляется на основе отраслевых документов стратегического планирования Российской Федерации. В целях актуализации таких документов Советом Безопасности Российской Федерации определяется перечень приоритетных направлений обеспечения информационной безопасности на среднесрочную перспективу с учетом положений стратегического прогноза Российской Федерации.

38. Результаты мониторинга реализации настоящей Доктрины отражаются в ежегодном докладе Секретаря Совета Безопасности Российской Федерации Президенту Российской Федерации о состоянии национальной безопасности и мерах по ее укреплению.

С полным документом Доктрины можно ознакомиться на сайтах.

7. МЕСТО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭКОНОМИЧЕСКИХ СИСТЕМ В НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СТРАНЫ

В современном мире информационная безопасность становится жизненно необходимым условием обеспечения интересов человека, общества и государства и важнейшим, стержневым, звеном системы национальной безопасности страны.

Доктрина национальной безопасности страны рассматривает всю работу в информационной сфере на основе и в интересах Концепции национальной безопасности РФ.

Доктрина выделяет четыре основные составляющие национальных интересов России в информационной сфере.

Первая составляющая включает соблюдение конституционных прав и свобод человека и гражданина в области получения и пользования информацией, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Для ее реализации необходимо:

1) повысить эффективность использования информационной инфраструктуры в интересах общественного развития, консолидации российского общества, духовного возрождения многонационального народа страны;

2) усовершенствовать систему формирования, сохранения и рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала России;

3) 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;

4) 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;

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

6) гарантировать свободу массовой информации и запрет цензуры;

7) не допускать пропаганды и агитации, которые способствуют разжиганию социальной, расовой, национальной или религиозной ненависти и вражды;

8) 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 в информационной сфере включает информационное обеспечение государственной политики страны, связанное с доведением до российской и международной общественности достоверной информации о ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам. Для этого требуется:

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

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

Третья составляющая национальных интересов в информационной сфере включает развитие современных информационных технологий, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка этой продукцией и выход ее на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов.

Для достижения результата на этом направлении необходимо:

1) развивать и совершенствовать инфраструктуру единого информационного пространства России;

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

3) развивать производство в стране конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей этих средств и систем;

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

Четвертая составляющая национальных интересов в информационной сфере включает защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем.

В этих целях требуется:

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

2) интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля их эффективности;

3) обеспечить защиту сведений, составляющих государственную тайну;

4) расширять международное сотрудничество России в области безопасного использования информационных ресурсов, противодействия угрозе противоборства в информационной сфере.

ЛИТЕРАТУРА

1. Вострецова Е.В. Основы информационной безопасности: учебное пособие для студентов вузов. – Екатеринбург : Изд-во Урал. ун-та, 2019. – 204 с.

2. Гатчин Ю.А., Сухостат В.В., Куракин А.С., Донецкая Ю.В. Теория информационной безопасности и методология защиты информации – 2-е изд., испр. и доп. – СПб: Университет ИТМО, 2018. – 100 с.

3. Гафнер В.В. Информационная безопасность: учебное пособие в 2 ч. – Ч.1. ГОУ ВПО «Урал. гос. пед. ун-т». – Екатеринбург, 2009. – 155 с.

4. Груздева, Л.М. Основы информационной безопасности : учеб. пособие в двух частях. – Ч. 1 / Л. М. Груздева. – М. : Юридический институт МИИТа, 2017. – 101 с.

5. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.

6. Указ Президента РФ от 5 декабря 2016 г. № 646 “Об утверждении Доктрины информационной безопасности Российской Федерации”.

У ч е б н о е и з д а н и е

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОВРЕМЕННОМ МИРЕ

Учебно-методическое пособие

Составитель: **Контылева** Елена Александровна

В авторской редакции

Изд. № 37/2022. Объем 4,25 п.л. Усл. печ. л. 3,95. Уч.-изд. л. 4,17.
РИИЦМ ФГАОУ ВО «Севастопольский государственный университет»