

1 Предпосылки развития государственного управления в сфере информационной безопасности

Основные задачи государственных органов в сфере информационной безопасности, также как и во многих других сферах, связаны с охраной общественных интересов, предотвращением противоправной деятельности, а также с защитой информации, имеющей государственную важность (военных сведений, информации о космических и ядерных технологиях и пр.). При этом решение вопросов информационной безопасности в частном секторе экономики, как правило, является прерогативой самих частных компаний и организаций, а вмешательство государства в эту сферу должно быть минимизировано. Таким образом, на практике деятельность органов власти, как правило, концентрируется на решении вопросов информационной безопасности внутри отдельных сфер, которые считаются наиболее важными для обеспечения государственной безопасности и достижения политических целей: вооруженные силы, внешняя разведка, стратегические технологии (например, космические, атомные и военные), государственные финансы, общественная стабильность и некоторые другие. Решению вопросов информационной безопасности в других областях государственными органами, как правило, уделяется меньше внимания. Государственные органы могут решать определенные задачи информационной безопасности, не относящиеся напрямую к защите государственных информационных систем, в тех случаях, когда выгоды от государственного вмешательства существенно превышают затраты и решения, предлагаемые государством, не составляют конкуренции альтернативным решениям (услугам, технологиям, методикам и пр.), которые предлагаются (или потенциально могут быть предложены) частными компаниями.

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

Деятельность государства в сфере информационной безопасности, как правило, строится на более общих задачах государственной власти, таких как:

- обеспечение социально-экономического развития страны и устойчивости финансовой системы;
- сохранение государственной и политической стабильности в стране;
- сохранение и развитие демократических институтов общества, а также обеспечение прав и свобод граждан;
- сохранение суверенитета государства;
- укрепление законности и правопорядка;
- участие в жизни международного сообщества.

По своей природе факторы, определяющие состояние информационной безопасности и, соответственно, деятельность государства в этой сфере, подразделяются на:

- организационно-технические;
- политические;
- социально-экономические.

Организационная деятельность государства в сфере информационной безопасности, как правило, сводится к противодействию различным угрозам:

1) Внешним, таким как деятельность иностранных спецслужб и вооруженных сил, враждебная экономическая и техническая политика отдельных государств, агрессивные рыночные стратегии крупных международных корпораций и финансово-промышленных групп, незаконная деятельность международных преступных и террористических группировок и пр.

2) Внутренним, таким как деятельность криминальных структур в сфере обращения информации, неправомерные действия государственных

структур, халатность или целенаправленные нарушения, допускаемые гражданами и организациями при использовании информационных систем и обращении информации, нарушения в работе информационных и телекоммуникационных систем и пр.

Таким образом, деятельность государства в этой сфере направлена на нейтрализацию существующих угроз информационной безопасности с учетом всех факторов, воздействующих как на сами управляющие государственные структуры, так и на информационные системы.

2 Общая методология и структура организационного обеспечения информационной безопасности на уровне государства

Для решения основных задач в сфере информационной безопасности действуют все основные органы государственной власти и управления: судебные, органы исполнительной власти, правоохранительные органы, организации и предприятия, которые контролируются государством и имеют доступ к информации, составляющей государственную тайну, и пр.

Для обеспечения информационной безопасности государственные органы выполняют следующие основные функции:

1) Выполняют судебные функции в отношении лиц, которые допустили правонарушения, связанные с использованием информационных ресурсов, и участвуют в хозяйственных спорах, связанных с нарушениями информационной безопасности.

2) Осуществляют правоприменительную деятельность, непосредственно реализуют меры по защите информационных ресурсов государственного управления, а также выполняют все функции, необходимые для реализации требований законодательства.

3) Создают законодательную базу, обеспечивающую защиту базовых прав частных лиц, предприятий и государства, таких как право на защиту частной информации, право на защиту коммерческой и банковской тайны,

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

право на беспрепятственный доступ к информации и пр. Данная функция осуществляется законодательными органами в сотрудничестве с органами исполнительной власти, общественными организациями, научно-исследовательскими учреждениями и другими заинтересованными участниками.

Функции создания и постоянного совершенствования законодательно-правовой базы, обеспечивающей защиту законных частных, коммерческих, общественных и государственных интересов, реализуются законодательными органами (парламентами) государств. Как правило, все законодательные функции в данной сфере в большинстве стран осуществляются центральными (федеральными) органами законодательной власти, а местные (региональные) органы таких полномочий не имеют. Для создания и поддержания в актуальном состоянии законодательства в сфере информационной безопасности в законодательных органах могут создаваться профильные комитеты и комиссии, которые состоят из членов данного законодательного органа, имеющих некоторые базовые знания и навыки в сфере информационных технологий и правового регулирования вопросов информационного обмена. Кроме того, вопросы совершенствования законодательства в сфере обеспечения информационной безопасности также могут решаться в различных профильных комитетах, подкомитетах и рабочих группах, специализирующихся на смежных проблемах государственного управления и социально-экономического регулирования, таких как:

- наука и образование;
- национальная безопасность;
- оборона;
- политика в сфере связи, информации и информатизации;
- промышленная и экономическая политика и пр.

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

Для разработки соответствующих нормативно-правовых актов подразделения (комитеты и подкомитеты) органов законодательной власти могут привлекать для совместной работы ответственных специалистов, руководителей, аналитиков и экспертов, работающих в:

- 1) Научно-исследовательских организациях, специализирующихся на соответствующих проблемах информационных технологий и управления.
- 2) Органах исполнительной власти (министерствах, отвечающих за научное и техническое развитие, т.н. «силовых» министерствах и ведомствах, юридических ведомствах и пр.).
- 3) Частных предприятиях, а также общественных и профессиональных организациях, которые занимаются оказанием информационных услуг, поставкой информационно-технических продуктов, специализирующихся на развитии информационных технологий и пр.

Процедуры согласования, принятия и утверждения законодательных актов, а также процедуры контроля за действиями органов исполнительной власти в каждой стране определяются в соответствии с действующим законодательством (конституцией).

Деятельность исполнительных органов государственной власти в сфере обеспечения информационной безопасности направлена на реализацию действующих в государстве законов и непосредственную защиту интересов государственной власти, гражданских прав и прав компаний, осуществляющих хозяйственную деятельность.

Конкретная работа органов исполнительной власти в сфере информационной безопасности, как правило, осуществляется по нескольким относительно самостоятельным направлениям:

- 1) Лицензирование и сертификация предприятий и организаций, занимающихся производством, продажей установкой и настройкой программных и аппаратных средств защиты информации.

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

2) Непосредственное осуществление функций защиты информации в государственных учреждениях и службах (правительство, вооруженные силы, органы внутренних дел и пр.).

3) Осуществление международного сотрудничества в сфере защиты информации (взаимодействие с правительствами и правоохранительными органами пр. стран) как в целях общего развития инфраструктуры информационной безопасности, так и для разрешения отдельных инцидентов (раскрытия преступлений и пр.).

4) Осуществление правоохранительной деятельности в сфере защиты информации (уголовного преследования лиц и преступных группировок, совершающих противоправные действия, содержащие признаки уголовных преступлений в соответствии с действующим уголовным законодательством).

5) Поддержка научных исследований в сфере информационной безопасности.

6) Поддержка образования и подготовки кадров, а также регулирование деятельности образовательных учреждений (включая установку образовательных стандартов).

7) Разработка государственных стандартов, относящихся к организации и технологиям защиты информации (программным и аппаратным средствам, средствам криптографии и пр.).

8) Установление конкретных правил производства, продажи, экспорта, импорта и использования средств защиты информации, а также организация системы контроля за соблюдением действующих законов и установленных правил.

Судебные функции, как правило, реализуются судами общей юрисдикции, так же, как и для всех остальных гражданских и уголовных дел. Специальных судебных инстанций, которые были бы предназначены для

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

рассмотрения дел, связанных с информационной безопасностью (таких как, например, суды по правам человека или военные суды), не существует. При этом могут создаваться судебные лаборатории, специализирующиеся на проведении экспертиз, анализов и исследований различных элементов информационных систем в связи с расследованиями и судебными разбирательствами по делам о нарушениях в сфере информационной безопасности.

Основой организации государственной деятельности в сфере информационной безопасности является национальная политика (доктрина, национальный план, национальная стратегия) информационной безопасности. Этот документ, издаваемый, как правило, главой исполнительной ветви власти (президентом страны) отражает:

- основные направления, в которых государство намерено осуществлять активные действия с целью повышения уровня информационной безопасности на национальном уровне (создание систем безопасности, упорядочивание взаимоотношений различных субъектов, пресечение правонарушений, развитие инфраструктуры и технологий безопасности и пр.):

- признание государственной властью существенной значимости проблем защиты информации для общества, личности, экономики и самого государства;

- современное понимание общего ландшафта информационной безопасности на национальном уровне: потенциально уязвимые информационные объекты, источники угроз и пр.

В рамках утвержденной государственной доктрины информационной безопасности:

- 1) Отдельные правительственные учреждения наделяются специфическими функциями и полномочиями, связанными с управлением

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

информационной безопасностью (как в общегосударственном масштабе, так и в рамках определенных сфер ответственности), а также создаются специальные структурные подразделения, отвечающие за решение вопросов защиты информации и информационной инфраструктуры.

2) Создается система локальных правовых актов, регулирующих отношения в сфере защиты информации, а также система государственных стандартов, относящихся к технологиям и организации защиты информации.

3) Создаются специализированные правительственные организации, отвечающие за реализацию политики информационной безопасности и решение отдельных задач в этой сфере.

Специализированные органы, создаваемые в структуре исполнительной власти для решения задач информационной безопасности на государственном уровне, как правило, подчиняются непосредственно главе исполнительной ветви власти, носят статус федеральных агентств, комитетов или комиссий и наделены правом самостоятельно издавать нормативные акты в рамках имеющихся полномочий, установленных действующим законодательством. Издаваемые таким образом локальные нормативные акты (указы, постановления, инструкции, порядки, правила и пр.) непосредственно регулируют отношения в сфере создания, распространения и использования средств автоматизации и защиты информации.

Государственная стандартизация технологий и методов, используемых в процессах защиты информации, осуществляется уполномоченными государственными органами с целью упорядочивания знаний о современном состоянии технологий и методов защиты и установления универсальных критериев надежности и функциональности для определенных технологий.

Государственная стандартизация позволяет достичь универсальности при оценке используемых технологий и методов и, таким образом, до

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

определенной степени упорядочить многие взаимоотношения, связанные с использованием таких технологий и методов.

Стандартизация, осуществляемая отдельными государственными органами, как правило, опирается на существующую систему имеющихся международных стандартов, а национальные органы, занимающиеся стандартизацией, могут принимать участие в разработке международных стандартов. Основными объектами государственной и международной стандартизации могут выступать:

- методы аутентификации;
- методы тестирования (проверки) и оценки информационных систем на предмет их защищенности;
- методы шифрования и криптографической защиты данных;
- некоторые другие элементы систем обеспечения информационной безопасности;
- технологии идентификации пользователей информационных систем.

3 Общая политика РФ в сфере информационной безопасности

Основой современной политики РФ в сфере информационной безопасности можно считать «Доктрину информационной безопасности РФ», утвержденную Президентом РФ В.В. Путиным 05.12. 2016 г. Этот документ:

- описывает основные направления международного сотрудничества в сфере информационной безопасности;
- описывает основные предпосылки формирования государственной политики в данной сфере (потребность в безопасности, существующие интересы, угрозы, источники угроз и пр.);
- описывает распределение ответственности между основными органами государственной власти, решающими задачи в сфере информационной безопасности;
- описывает состояние дел в сфере общегосударственного регулирования процессов информационной безопасности на момент утверждения Доктрины (основные достижения и недостатки);
- перечисляет основные информационные объекты (в различных сферах), на охрану которых должна быть направлена государственная политика;
- перечисляет основные организационные инструменты, используемые для реализации государственной политики и осуществления государственного управления в сфере информационной безопасности;
- перечисляет приоритетные направления деятельности государства (задачи, требующие безотлагательного решения) по обеспечению информационной безопасности;
- формулирует базовые задачи государства и общества, основанные непосредственно на необходимости выполнения требований Конституции, обеспечения суверенитета страны и пр.;

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

– формулирует основные методики, которые государство должно использовать для обеспечения информационной безопасности, а также специфику применения этих методов в отдельных областях общественной жизни.

В соответствии с Доктриной государство должно уделять внимание информационной безопасности в таких основных сферах, как:

- внешняя политика;
- внутренняя политика;
- духовная жизнь;
- информационные системы государственного управления;
- наука и техника;
- оборона;
- экономика.

К числу первоочередных мероприятий, которые должны быть реализованы на государственном уровне, Доктрина относит:

- подготовку кадров для работы в сфере информационной безопасности;
- принятие и реализацию федеральных программ, решающих определенные задачи информатизации и обеспечения информационной безопасности: создание информационных архивов и информационно-телекоммуникационных систем органов власти, развитие информационной культуры населения;
- разработку механизмов управления государственными средствами массовой информации и реализации государственной информационной политики;
- совершенствование законодательной базы в сфере информационных отношений;

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

– совершенствование и развитие системы государственных стандартов в сфере информатизации и обеспечения информационной безопасности и пр.

Как можно видеть из этого перечня, а также в целом из текста Доктрины, она предполагает определенное расширение понятия «информационная безопасность» и включение в него некоторых вопросов, которые связаны с деятельностью средств массовой информации и другими аспектами информационной политики, не имеющими прямого отношения к категории «информационная безопасность» в ее первоначальном понимании.

Помимо Доктрины также важным основополагающим документом, в значительной мере определяющим политику государства в сфере информатизации и обеспечения защиты информации, можно считать Федеральную целевую программу «Электронная Россия», реализация которой планируется в три этапа в период с 2002 по 2010 год. В частности, одной из заявленных целей реализации данной Программы является обеспечение реализации прав на «обеспечение конфиденциальности любой охраняемой законом информации, имеющейся в информационных системах». В целом предполагается, что весь комплекс мероприятий, предусмотренных Программой, должен обеспечить принципиально более высокий уровень надежности ключевых информационных потоков на государственном уровне.

Кроме того, важными организующими документами, действующими в этой сфере на государственном уровне, являются:

- 1) Федеральный Закон «О государственной тайне».
- 2) Федеральный Закон «Об информации, информационных технологиях и о защите информации».
- 3) Федеральный Закон «Об участии в международном информационном обмене».

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

Структура органов государственной власти, обеспечивающих информационную безопасность в РФ:

1) Важную роль в системе органов государственной власти, отвечающих за решение задач информационной безопасности, играет также Служба специальной связи и информации («Спецсвязь РФ»), с 2004 года входящая в состав Федеральной службы охраны.

2) Ведущим государственным учреждением, непосредственно ответственным за реализацию государственной политики в сфере информационной безопасности и защиту государственных интересов на общенациональном уровне, является Федеральная служба по техническому и экспортному контролю – ФСТЭК.

3) Основным государственным органом, определяющим политику РФ в сфере безопасности страны в целом и информационной безопасности в частности, является Совет безопасности РФ.

Вопросы повышения качества информационной работы и информационной безопасности решают также другие федеральные органы (в пределах своей компетенции):

- 1) Министерство внутренних дел РФ.
- 2) Министерство связи и массовых коммуникаций РФ;

Также отдельные государственные ведомства, предъявляющие особые требования к уровню защищенности информации, реализуют собственные мероприятия по обеспечению защиты информации:

- 1) ФСБ (Управление компьютерной и информационной безопасности, а также Центр по лицензированию, сертификации и защите государственной тайны, Управление специальной связи и НИИ информационных технологий);
- 2) Минатом РФ и система подведомственных ему предприятий (в составе которого функционирует Центр «Атомзащитаинформ»);

3) Центральный банк РФ (в составе которого функционирует Главное управление безопасности и защиты информации) и пр.

Совет Безопасности РФ, возглавляемый Президентом РФ, состоит из ключевых министров и рассматривает вопросы внутренней и внешней политики РФ в области обеспечения безопасности, стратегические проблемы государственной, экономической, общественной, оборонной, информационной, экологической и иных видов безопасности. Основными функциями Совета Безопасности являются:

- подготовка решений Президента РФ по соответствующим вопросам, в т.ч. по вопросам информационной безопасности;
- рассмотрение законопроектов, в рамках своей компетенции;
- организация и координация разработки стратегии в области внутренней, внешней и военной политики, военно-технического сотрудничества и информационной безопасности РФ;
- осуществление контроля за реализацией этой стратегии органами власти, оценка внутренних и внешних угроз жизненно важным интересам объектов безопасности и выявление их источников и пр.

Для решения задач, связанных с обеспечением информационной безопасности, в составе СБ функционирует созданное в 1997 году Управление информационной безопасности (одно из восьми профильных управлений), а также Межведомственная комиссия по информационной безопасности. Функциями Управления информационной безопасности являются:

- анализ и прогнозирование ситуации в области информационной безопасности РФ;
- выявление источников опасности, оценка внешних и внутренних угроз информационной безопасности и подготовка предложений Совету Безопасности по их предотвращению;

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

- подготовка предложений по проектам решений Совета Безопасности и информационно-аналитических материалов к его заседаниям по вопросам обеспечения информационной безопасности РФ;
- подготовка предложений Совету Безопасности по выработке и реализации основных направлений политики государства в области обеспечения информационной безопасности РФ;
- подготовка предложений Совету Безопасности по разработке проектов нормативных правовых актов, направленных на обеспечение информационной безопасности РФ;
- рассмотрение в установленном порядке проектов федеральных целевых программ, направленных на обеспечение информационной безопасности РФ, подготовка соответствующих предложений;
- участие в подготовке материалов по вопросам обеспечения информационной безопасности РФ для ежегодного послания Президента РФ Федеральному Собранию и для докладов Президента РФ.

Федеральная служба по техническому и экспортному контролю (ФСТЭК), до августа 2004 года известная как Государственная техническая комиссия при Президенте РФ (Гостехкомиссия РФ), была создана в январе 1992 года на базе Гостехкомиссии СССР по противодействию иностранным технологическим разведкам, которая, в свою очередь ведет отсчет своего существования с декабря 1973 года.

Произошедшее в 1992 году преобразование было связано со сменой политических приоритетов, интенсивным развитием электронных коммуникаций и средств вычислительной техники, отменой государственной монополии на многие сферы экономической и технической деятельности, развитием рыночных отношений, расширением международных связей и другими факторами. ФСТЭК, ранее подчинявшаяся напрямую Президенту РФ, в процессе административной реформы была подчинена Министерству

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

обороны. ФСТЭК является коллегиальным органом – в состав Коллегии входят около двадцати представителей различных министерств и ведомств (главным образом, в ранге заместителей министров и директоров департаментов), таких как МВД, МИД, ФСБ, Минатом, ФСО, СВР и пр.

Основными функциями ФСТЭК являются:

- организация и контроль за проведением работ по защите информации в органах государственного управления, объединениях, концернах, на предприятиях, в организациях и учреждениях (независимо от форм собственности) от утечки по техническим каналам, от несанкционированного доступа к информации, обрабатываемой техническими средствами, и от специальных воздействий на информацию с целью ее уничтожения и искажения;
- поддержание системы лицензирования деятельности предприятий, организаций и учреждений по осуществлению мероприятий и (или) оказанию услуг в области защиты информации и сертификации средств защиты информации;
- проведение единой технической политики и координация работ по защите информации;

Для реализации функций по лицензированию в составе ФСТЭК функционируют 7 региональных управлений (по федеральным округам), а также 20 отраслевых аттестационных (лицензионных) центров.

Служба специальной связи и информации (Спецсвязь РФ), созданная в марте 2003 года в рамках Федеральной службы охраны на базе упраздненного Федерального агентства правительственной связи и информации (ФАПСИ), в целом призвана обеспечивать функционирование президентской связи, организацию, эксплуатацию и развитие специальной связи для государственных органов и решать другие аналогичные задачи.

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

При этом задачами Спецсвязи также являются:

- выполнение требований обеспечения информационной безопасности объектов государственной охраны;
- организация в системе специальной связи шифровальной деятельности, отнесенной к компетенции Спецсвязи РФ;
- организация и проведение мероприятий по предотвращению утечки по техническим каналам информации в системах специальной связи, информационно-технологических, информационно-аналитических и информационно-телекоммуникационных системах, находящихся в ведении Спецсвязи РФ;
- проведение работ по защите технических средств специальной связи, устанавливаемых в категорированных помещениях государственных органов, включая особо важные;
- участие в разработке и реализации мер по обеспечению информационной безопасности Российской Федерации, защите сведений, составляющих государственную тайну;
- участие в разработке нормативной технической документации по вопросам защиты информации в системах специальной связи;
- участие в создании, обеспечении и развитии системы электронного документооборота государственных органов с использованием удостоверяющих центров.

Министерство связи и массовых коммуникаций РФ в лице подчиняющегося ему Федерального агентства по информационным технологиям (Росинформтехнологии) осуществляет и организует следующие виды работ в сфере информационной безопасности:

- ведение единого государственного реестра сертификатов ключей подписей удостоверяющих центров и реестра сертификатов ключей подписей уполномоченных лиц федеральных органов государственной власти, а также

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

обеспечение доступа к ним граждан, организаций, органов государственной власти и органов местного самоуправления;

- выполнение функции государственного заказчика научно-технических и инвестиционных программ и проектов в сфере информационных технологий;

- подтверждение подлинности электронных подписей уполномоченных лиц удостоверяющих центров в выданных ими сертификатах ключей подписей.

Уполномоченным органом по ведению реестра доверенных удостоверяющих центров является ФГУП НИИ «Восход».

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) является уполномоченным федеральным органом исполнительной власти по защите прав субъектов персональных данных. В полномочия данного органа входит пресечение нарушений, которые могут возникать при обработке персональных данных граждан РФ.

В системе законодательной власти основным структурным подразделением, призванным решать вопросы формирования и реализации государственной политики в сфере информационной безопасности, является Комитет по безопасности Государственной думы Федерального собрания Российской Федерации. В составе этого Комитета функционирует Подкомитет по информационной безопасности. В законодательной работе в рамках этого Комитета принимают участие:

- представители ведущих научно-исследовательских учреждений и учебных заведений;

- представители крупных коммерческих компаний – лидеров в развитии организации и технологий информационной безопасности (в том числе банков, технологических компаний и пр.);

Тема 2.2 – Планирование и управление информационной безопасностью на государственном уровне: общие принципы и российская практика
(Планирование и управление информационной безопасностью)

- представители общественных организаций, фондов и профессиональных объединений;
- руководители Совета безопасности РФ и пр. правительственных органов;
- специалисты и руководители профильных подразделений ФСБ, СВР, ФСТЭК, МВД и пр. ведомств.