# Система обеспечения информационной безопасности.

## Обеспечение информационной безопасности организации

При всем многообразии видов организаций, направлений и масштабов их деятельности, численности участников основными объектами обеспечения информационной безопасности, как правило, являются:

* информация в форме сведений (сведения об участниках организации, о состоянии рынка и ее активов; репутация организации и доброе имя участников организации и т.п.);
* информация в форме сообщений (документы, закрепляющие права собственности организации на материальные и нематериальные активы; документация бухгалтерского учета, налоговые декларации, договоры на выполнение работ и оказание услуг, документация на выпускаемые изделия и т.п.);
* информационная инфраструктура (автоматизированные системы обработки информации и технологического управления; техническое и программное обеспечение информационных и коммуникационных систем и сетей связи, используемых в организации, и т.п.);
* правовой статус организации как субъекта информационной сферы (права на объекты интеллектуальной собственности, на выполнение работ и оказание услуг, на доступ к открытой информации государственных органов, на коммерческую тайн} и т.п., а также обязанности по представлению в уполномоченные государственные органы сведений о результатах экономической деятельности, по соблюдению режима персональных данных, по представлению заинтересованным лицам документов в случае направления заявки на участие в конкурсах и аукционах и т.п.).

Наиболее опасные угрозы безопасности этих объектов проявляются в следующих формах:

* мошенничество, связанное с завладением чужим имуществом или приобретением права на него путем обмана или злоупотребления доверием, основанных на неправомерном доступе к информационно-коммуникационным системам, конфиденциальной информации, на подделке или искажении электронных документов в информационных и коммуникационных системах, сетях;
* клевета, основанная на распространении заведомо ложной информации, порочащей честь и достоинство руководителей организации;
* нарушение авторских и смежных прав, связанных с объектами интеллектуальной собственности;
* шантаж, связанный с угрозой распространения персональных данных, иной информации, охраняемой законом в режиме тайны;
* противоправное раскрытие информации ограниченного доступа третьим лицам;
* уничтожение или повреждение информационных ресурсов, информационно-коммуникационных систем и сетей связи посредством использования и распространения вредоносных программ, нарушения правил эксплуатации ЭВМ и их сетей;
* причинение имущественного ущерба собственнику или иному владельцу информационно-коммуникационных систем и сетей связи путем обмана или злоупотребления доверием без признаков хищения.

Вследствие проявления указанных угроз существенно возрастают риски, связанные с осуществлением основной деятельностиорганизации (риск утраты репутации, риск ликвидности, операционные риски, риски утраты собственности или важных активов организации). Эти риски связаны с возможностью возник­новения ситуаций проявления угроз, требующих дополнительных,часто существенных затрат материальных, людских, временных, финансовых и иных ресурсов на ликвидацию последствий проявления угроз. Увеличение рисков приводит к увеличению издержек и соответствующему снижению эффективности деятельности организации, уменьшению ее конкурентоспособности.

Система обеспечения информационной безопасности организации характеризуется двумя составляющими: деятельностью по подготовке и реализации мер, направленных на противодействие проявлению угроз информационной безопасности и минимизацию последствий этих проявлений; субъектами этой деятельности.

Деятельность по обеспечению информационной безопасности базируется на следующих основных принципах:

законность, заключающаяся в строгом и неуклонном исполнениинорм законодательства Российской Федерации, соблюдении прав и свобод человека и гражданина;

непрерывность, предполагающая рассмотрение деятельности в качестве одной из функций организации;

комплексность, заключающаяся во всестороннем анализе фактов оказывающих влияние на риски информационной безвинности, при планировании данной деятельности и использовании всех имеющихся возможностей и выделенных ресурсов для реализации составленных планов;

замкнутость, заключающаяся в совместном осуществлении деятельности по предупреждению проявления угроз, снижению их опасности, выявлению проявлений угроз, минимизации последствий этих проявлений, а также по оценке эффективности выполнения планов противодействия угрозам и их соответству­ющего уточнения.

В этой деятельности широко используются методы поощрения, убеждения и принуждения.

Меры по противодействию проявлению угроз информационной безопасности организации и минимизации последствий этих проявлений охватывают три основных направления деятельности:

* управление персоналом;
* организация объектового режима;
* организационно-техническое обеспечение.

Меры по управлению персоналом направлены на минимизацию рисков, связанных с проявлением личностных свойств и качеств участников организации, а также взаимодействующих с ней субъектов. Они включают подбор и расстановку кадров, обеспечение должной мотивации сотрудников к добросовестной работе, подготовку и повышение их квалификации.

Меры по организации объектового режима нацелены на минимизацию рисков, связанных с возможными попытками нанесения ущерба организации ее участникам и взаимодействующим с ней субъектам. Эти мероприятия включают осуществление пропускного и внутриобъектового режимов, в том числе установ­ление и поддержание режимов информации, информационно- коммуникационных систем и систем связи, контроль поддержания установленных режимов и проведение служебных расследований по фактам их нарушения. При этом режимы информационно-коммуникационных систем и систем связи направлены на достижение требуемых значений основных свойств безопасности используемых в организации информационных технологий: конфиденциальности, целостности и готовности к использованию.

Меры по организационно-техническому обеспечению позволяют использовать возможности техники для установления и поддержания объектового режима. Они включают мероприятия по использованию средств защиты информации, информационных и коммуникационных систем, средств связи, а также по установлению и реализации политики безопасности в информационно-коммуникационных системах.

Важную роль в эффективной реализации мер по противодействию угрозам информационной безопасности играет нормативно-методическое обеспечение.

Субъектами обеспечения информационной безопасности организаций являются создаваемые в них координационные (например, советы по безопасности информационных технологий) и кадровые органы, специализированные структурные подразделения по вопросам информационной безопасности или должностные лица, а также структурные образования, специализирующиеся на оказании услуг в данной области, объединяемые в единую систему.

Структура указанной системы и ее составных частей может быть различной. Например, в организации может быть создан совет по безопасности информационных технологий, который решает вопросы выработки внутренней политики в этой области, ее реализации и нормативно-методического обеспечения.

Для качественного выполнения данных функций в состав совета включают представителей высшего руководства организации и должностных лиц, осуществляющих непосредственное управление обеспечением информационной безопасности. В некоторых случаях управление этой деятельностью может быть возложено на ответственных сотрудников соответствующих структурных подраз­делений.

## Обеспечение информационной безопасности Российской Федерации

Осуществление деятельности по обеспечению информационной безопасности Российской Федерации возложено на государство, которое в соответствии с законодательством является основным субъектом обеспечения безопасности.

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

В соответствии с Доктриной информационной безопасности Российской Федерации национальные интересы в информационной сфере включают следующие основные составляющие:

* соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны;

-информационное обеспечение государственной политики Российской Федерации;

* развитие современных информационных технологий, отечественной индустрии информации, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на Мировой рынок; обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов;
* защита национальных информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем.

Основными объектами обеспечения информационной безопасности Российской Федерации являются ее национальные интересы:

* информация в форме сведений (свобода мысли, национальные культурные ценности);
* информация в форме сообщений (архивные документы; документы, являющиеся музейными предметами или составляющие музейные коллекции; тиражированные документы);
* информационная инфраструктура (сети связи и инфраструктура информатизации; инфраструктура средств массовой информации и книгоиздания; инфраструктура открытых информационных ресурсов библиотек, архивных и музейных фондов);
* правовой статус субъектов информационной сферы Российской Федерации (совокупность реальных прав и обязанностей субъектов).

К угрозам информационной безопасности Российской Федерации, в частности, относятся:

* противодействие реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;
* противоправные сбор и использование информации;
* разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
* уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
* утечка информации по техническим каналам;
* внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;
* уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
* перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
* использование не сертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи.

**-** создании и развитии российской информационной инфраструктуры;

* несанкционированный доступ к информации, находящейся в банках и базах данных;
* нарушение законных ограничений на распространение информации.

Деятельность по обеспечению информационной безопасности Российской Федерации осуществляется на основе принципов, разделяемых на общие и особенные.

К наиболее важным общим принципам деятельности по обеспечению безопасности относятся гуманизм, конкретность, эффективность, сочетание гласности и профессиональной тайны, законность и конституционность.

Принцип гуманизма заключается в обеспечении прав и свобод человека и гражданина при осуществлении противодействия угрозам информационной безопасности, недопущении противоправных посягательств на его личность, унижения чести и достоинства человека, произвольного вмешательства в его частную жизнь, личную и семейную тайны, ограничения свободы его информационной деятельности, а также в минимизации ущерба этим правам и свободам в случаях, когда их ограничение осуществляется на законных основаниях.

Принцип конкретности состоит в обеспечении безопасности применительно к конкретным жизненным обстоятельствам с учетом разнообразных форм проявления объективных законов на основе достоверной информации как о внутренних и внешних угрозах, так и о возможностях противодействия им. Достоверная информация позволяет установить конкретные формы проявле­нияугроз, определить в соответствии с этим цели и действия по обеспечению безопасности, конкретизировать методы противодействия угрозам, а также необходимые для их реализации силы и средства.

Принцип эффективности заключается в достижении целей про­тиводействия при наименьших затратах сил и средств. Обеспечение информационной безопасности в любой социальной общности требует определенных материальных, финансовых и людских Ресурсов. Исходя из этого обеспечение безопасности, как и всякая общественно полезная деятельность людей, должно осуществляться рационально и эффективно.

Принцип сочетания гласности и профессиональной тайны состоит в нахождении и поддержании необходимого баланса между открытостью деятельности по противодействию угрозам информационной безопасности, позволяющей добиться доверия и поддержки общества, и защитой определенной информации, разглашение которой может снизить эффективность противодействия угрозам безопасности.

Принцип законности и конституционности означает осуществление всех свойственных государственным организациям и должностным лицам функций в строгом соответствии с действующей конституцией, законами и подзаконными актами, согласно установленной в законодательном порядке компетенции. Строгое и неуклонное соблюдение законности и конституционности долж­но быть непременным требованием, принципом деятельности не только государственных, но и негосударственных органов, учреждений и организаций.

К числу особенных принципов деятельности по обеспечению информационной безопасности следует отнести прежде всего глобальность.

Принцип глобальности заключается в том, что указанная деятельность должна осуществляться согласованно как в конкретном обществе, так и в международном сообществе. К важным формам осуществления деятельности по обеспечению информационной безопасности относится социальное регулирование, в том числе правовые и организационные мероприятия.

Важнейшими формами осуществления деятельности по обеспечению информационной безопасности являются регулятивная и организационная формы.

Регулятивная форма деятельности по обеспечению информационной безопасности характеризуется нормами регулирования общественных отношений по поводу противодействия угрозам и мерами по выработке и поддержанию этих норм. Выделяют два основных типа норм: технические и социальные.

• Технические нормы определяют порядок взаимодействия человека с окружающей средой, осуществления деятельности по созданию материальных благ, пользования орудиями труда, в частности средствами и системами информатизации, телекоммуникации и связи. Современную систему технических норм составляют правила использования современных информационных технологий, правила защиты информации и информационных систем от несанкционированного доступа, правила пользования средствами автоматизации управления и обработки информации. Следование этим правилам способствует более производительной и эффективной работе, предупреждает нанесение ущерба таким объектам национальных интересов, как информация и информационно-телекоммуникационные системы, производственный травматизм и заболевания.

• Социальные нормы регулируют поведение индивидов и подразделяются на поддерживаемые силами социальной общности без участия государства и на поддерживаемые с использованием государственного принуждения.

Первые включают прежде всего мораль, обычаи и традиции, корпоративные и религиозные нормы. Эти нормы играют большую роль в противодействии угрозам сохранения национальной идентичности.

• Мораль, или моральные нормы, — правила поведения, основанные на представлениях национальной общности о добре и зле, справедливости и несправедливости, честности и бесчестии и других подобных этических качествах. Значительная часть моральных норм вырабатывается и поддерживается нацией в целом или большей частью ее социальных групп.

Под обычаями понимаются правила поведения, сложившиеся в далеком прошлом и поддерживаемые в силу привычки в современном обществе. Норма, ставшая обычаем, оказывает свое регулирующее воздействие в силу ее эмоционального восприятия членами общества, привыкшими к ее соблюдению настолько, что реализация данной нормы превратилась в потребность.

Традиции представляют собой правила поведения, которые определяют порядок, процедуру проведения каких-либо мероприятий, связанных с торжественными или знаменательными, значительными событиями в жизни индивида как представителя конкретной нации, а также другие элементы социального и культурного наследия, передающиеся от поколения к поколению (идеи, Взгляды, вкусы, образ действия и мысли и т.п.).

Широкое распространение в современном обществе получили нормы общественных объединений, политических партий, закрепленные их уставами, **-** корпоративные нормы. Эти нормы определяют порядок участия членов в деятельности конкретных организаций, их взаимоотношения с руководством, взаимодействие с другими организациями.

Религиозные нормы представляют собой правила, установленные различными вероисповеданиями. Такие нормы содержатся в Библии, Коране, Талмуде и других религиозных книгах либо в сознании верующих, исповедующих языческие, многобожеские культы.

Важной составляющей социального регулирования деятельности по обеспечению информационной безопасности является праворегулирование общественных отношений. Оно заключается в установлении определенных правовых норм осуществления наиболее важных общественных отношений и охраны этих норм от нарушения с использованием государственного принуждения. Правовое регулирование отношений в целях обеспечения информационной безопасности осуществляется в рамках правовой деятельности государства, в структуре которой выделяются законодательная (правотворческая), правоприменительная и судебная деятельность.

Законодательная деятельность заключается в подготовке, принятии и издании законодательными органами нормативных правовых актов, регулирующих отношения в области удовлетворения национальных интересов в информационной сфере, а также создающих условия для предотвращения реализации угроз информационной безопасности или минимизации их воздействия на защищаемые общественные отношения. Законодательная деятельность направлена на создание правовой основы выполнения государственными органами задач по противодействию угрозам, на установление таких правил реализации общественных отношений в рассматриваемой области, при которых ни внешние, ни внутренние угрозы не оказывают на защищаемые отношения существенного негативного воздействия. Совокупность нормативных правовых актов, являющихся источниками права в данной сфере, составляют основу так называемого нормативного правового обеспечения информационной безопасности.

Правоприменительная деятельность представляет собой основанную на законодательстве оперативную, повседневную реализацию органами исполнительной власти (государственного управления) функций государства в области обеспечения информационной безопасности. Эта деятельность осуществляется в следующих формах:

* подготовка, принятие и исполнение решений органов исполнительной власти об осуществлении конкретных мероприятий по противодействию угрозам информационной безопасности;
* координация деятельности органов исполнительной власти в процессе подготовки и реализации конкретных мероприятий;
* осуществление правоприменительной практики в рассматриваемой области;
* проведение консультативной и информационной деятельности органов исполнительной власти, направленной на создание условий для эффективного выполнения возложенных на эти органы задач;
* выполнение учетной, аналитической, прогнозной и программной работы, административных договоров;
* взаимодействие органов исполнительной власти с другими ветвями и институтами государственной власти в целях согласования усилий по противодействию угрозам;
* информационное обеспечение всех субъектов противодействия угрозам информационной безопасности в системе исполнительной власти;

- государственный контроль за законностью деятельности субъектов правового регулирования в рассматриваемой области.

Судебная деятельность охватывает реализацию функции государства по обеспечению правосудия в процессе выполнения задач противодействия угрозам информационной безопасности. Эта деятельность является неотъемлемой составляющей обеспечения информационной безопасности, так как позволяет каждому реализовать свое конституционное право на объективное рассмотрение всех обстоятельств, связанных с применением к нему мер государственного принуждения.

Правовое обеспечение информационной безопасности характеризуется двумя основными составляющими: деятельностью государства по обеспечению информационной безопасности, осуществляемой в правовой форме; органами государственной власти, осуществляющими эту деятельность. Данное правовое обеспечение возникает в процессе взаимодействия права (как средства регули­рования общественных отношений) и государства (как основного субъекта противодействия угрозам его безопасности). Правовое обеспечение проявляется в воздействии правовых механизмов на общественные отношения в целях осуществления функций государства по противодействию угрозам безопасности.

Правовое обеспечение информационной безопасности регулирует отношения в области организации противодействия угрозам информационной безопасности как отдельных организаций, так и Российской Федерации в целом, во многом определяя структуру и принципы других видов обеспечения информационной безопасности, в частности организационного обеспечения.

Правовые средства обеспечения информационной безопасности выражаются в установлениях (субъективные права, обязанности, льготы, запреты, поощрения, наказания и т.п.) и деяниях (технологии — акты реализации прав и обязанностей), противодействующих реализуемым в информационной сфере угрозам интересам субъектов права и обеспечивающих достижение социально полезных целей. Они отражают функциональную, прикладную сторону правовой системы, выступают в качестве элементов механизма правового регулирования, во многом определяя эффективность данного механизма.

Организационное обеспечение информационной безопасности состоит в осуществлении планирования и управления материальными, людскими, финансовыми и другими ресурсами государства выделяемыми для противодействия угрозам. В рамках этой деятельности могут приниматься меры, направленные на развитие научных исследований в области повышения устойчивости информационной инфраструктуры к проявлению угроз, на содей­ствие в установленном законодательством порядке работе общественных организаций, ставящих своей целью противодействие угрозам информационной безопасности и определение форм возможного взаимодействия с ними, на согласование деятельности федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации в области про­тиводействия угрозам, на развитие системы массовой информации, способной удовлетворять потребности граждан в актуальных, достоверных сведениях об интересующих их событиях общественной жизни, обеспечивать их своевременное поступление к гражданам и т.д.

Организационное обеспечение информационной безопасности Российской Федерации осуществляется с использованием средств технического, кадрового, материального, финансового, информационного и научного обеспечения.

Средства технического обеспечения информационной безопасности образуются совокупностью технических и программных средств защиты информации, предотвращения несанкционированного доступа в информационные, телекоммуникационные и вычислительные системы и сети связи, а также методического обеспечения их использования.

Средства кадрового обеспечения информационной безопасности характеризуются программами подготовки кадров по различным аспектам данной деятельности, а также используемыми учебными и методическими материалами.

Средства материального обеспечения характеризуются совокупностью объектов, выделяемых для размещения средств технологического обеспечения, сил, участвующих в обеспечении информационной безопасности, средств организации их деятельности и т.п.

Средства финансового обеспечения представляют собой совокупность экономических инструментов получения, привлечения, перераспределения и использования денежных средств для решения задач обеспечения информационной безопасности.

Средства информационного обеспечения образуются совокупностью информационных фондов и банков данных, используемых в процессе решения задач обеспечения информационной безопасности, а также средств их актуализации.

Средства научного обеспечения информационной безопасности определяются совокупностью научных теорий, концепций, категорий, закономерностей и методов, предназначенных для изучения процессов и явлений развития информационной сферы общества, угроз национальным интересам, реализуемым в этой сфере, и для противодействия этим угрозам. Общая структура средств обеспечения информационной безопасности представлена на рис. 2.



Рис.2

Основные субъекты обеспечения информационной безопасности Российской Федерации объединены в рамках государственной системы защиты информации. К их числу относятся:

* службы контроля, надзора и обеспечения информационной безопасности государственных органов;
* специализированные предприятия и организации, осуществляющие деятельность в области разработки средств и предоставления услуг по защите информации;
* сертификационно - испытательные центры; аттестационные центры;
* службы безопасности и защиты информации предприятий и организаций, осуществляющих обработку персональных данных, конфиденциальной информации и информации, составляющей государственную тайну.