Тема 2. Организационно-правовая защита информации
Лекция 1. Государственная система защиты информации

Как было рассмотрено в предыдущей лекции, выделяются следующие ***направления*** защиты информации:

– ***правовая (законодательная) защита информации*** – защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением;

– ***организационная защита информации*** – реализующая меры организационного характера, предназначенные для регламентации функционирования информационных систем, работы персонала, взаимодействия пользователей с системой;

– ***инженерно-техническая защита*** – это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации. Она включает:

- ***физическая защита информации*** — защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты;
- ***техническая защита информации*** — защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств;
- ***криптографическая защита информации*** — защита информации с помощью ее криптографического преобразования.

Рассмотрим более подробно структуру государственной системы обеспечения информационной безопасности Российской Федерации и правовую или законодательную защиту информации.

1. Структура государственной системы обеспечения информационной безопасности Российской Федерации

Органы обеспечения информационной безопасности в совокупности с законодательством образуют ***государственную систему информационной безопасности и защиты информации.*** Государственная система защиты информации включает:

– органы законодательной, исполнительной и судебной властей;

– законодательство, регулирующее отношения в области защиты информации и информационных ресурсов;

– нормативную правовую базу по защите информации;

– службы (органы) защиты информации предприятий, организаций, учреждений.

Структура государственной системы защиты информации представлена на рис. 2.1.

Органы законодательной власти **(*Государственная дума*)** издают законы, регулирующие отношения в области защиты информации. Их перечень будет рассмотрен далее.

Нормативная база формируется на основе нормативных правовых актов в области защиты информации, издаваемых органами различных ветвей власти, министерствами, ведомствами. Основу нормативной базы составляют руководящие документы и стандарты, издаваемые Госстандартом.

***Органы исполнительной власти* (*правительство*)** контролируют исполнение этих законов. Правительство принимает соответствующие постановления в области защиты информации и издает распоряжения, являющиеся подзаконными нормативными правовыми актами.

Рис. 2.1. Государственная система защиты информации

Министерства и ***ведомства*** в соответствии со своим предназначением разрабатывают и принимают постановления и решения, являющиеся нормативными правовыми актами. Кроме того, они разрабатывают и утверждают такие нормативные акты, как положения, руководства, инструкции, правила, методические рекомендации. К нормативным актам этого уровня относятся также приказы и письма руководителей ведомств и министерств.

К основным ведомствам, регулирующим отношения в области защиты информации (регуляторам), относятся:

– Межведомственная комиссия по защите государственной тайны;
– Федеральная служба технического и экспортного контроля (ФСТЭК);
– Госстандарт России;
– Федеральная служба безопасности (ФСБ РФ).

Кроме этого, в обеспечении информационной безопасности принимают участие Служба внешней разведки России и Федеральная пограничная служба.

Основным органом управления государственной системы защиты информации является ФСТЭК. Для организации и осуществления защиты информации ФСТЭК издает соответствующие нормативные документы.

Госстандарт разрабатывает стандарты в области защиты информации.

Органы ФСБ РФ выполняют свои функции, будут рассмотрены далее.

Органы МВД ведут борьбу с правонарушителями в информационной сфере и компьютерными преступлениями. Для этого в структуре МВД создано специальное ***управление «Р»*** для предотвращения и раскрытия компьютерных преступлений.

Органы Государственного таможенного комитета (ГТК) обязаны предупреждать незаконный ввоз и вывоз из России «пиратской» продукции, обеспечивая тем самым защиту авторских и патентных прав.

Руководители предприятий, организаций, учреждений в соответствии со своими должностными обязанностями при деятельности, связанной с информацией, которая составляет государственную или иную тайну, создают службу (подразделение) по защите информации. Для организации соответствующей деятельности они издают нормативные правовые акты (приказы, распоряжения), а также утверждают руководства, инструкции, положения, правила, методические рекомендации, касающиеся защиты информации и деятельности служб защиты информации. Для деятельности, связанной с государственной тайной, предприятие должно иметь лицензию на этот вид деятельности, в его структуру вводится специальный отдел ФСБ; все средства защиты должны быть сертифицированы.

Судебная власть осуществляет надзор и привлечение к ответственности за нарушения законодательства в информационной сфере. В своей деятельности суды руководствуются соответствующими статьями УК РФ, ГК РФ, КОАП.

Итак, ***информационная безопасность*** является важной составляющей ***национальной безопасности России***. Политика государства в этой сфере деятельности направлена в первую очередь на организацию защиты государственной тайны и развитие правовых основ защиты информации. Правовая защита информации выступает как один из наиболее важных способов и методов защиты информации.

Вопрос 2. Основные законодательные акты в области информационной безопасности

Основные федеральные законы, касающиеся обеспечения безопасности информации, представлены далее.

Доктрина информационной безопасности Российской Федерации, введена в действие Указом Президента Российской Федерации 5.12.2016 г. №646 – документ, представляющий собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

Под информационной сферой в Доктрине понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «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.

Доктрина утверждена Указом Президента Российской Федерации от 5.12.2016 года № 646 и опубликована 6.12.2016 года.

Документ определяет национальные интересы России в информационной сфере:

−обеспечение и защита прав и свобод граждан в части получения и использования информации, неприкосновенность частной жизни, а также сохранение духовно-нравственных ценностей;

−бесперебойное функционирование критической информационной инфраструктуры (КИИ);

−развитие в России отрасли ИТ и электронной промышленности;

−доведение до российской и международной общественности достоверной информации о государственной политике РФ;

−содействие международной информационной безопасности.

В Доктрине перечисляются основные информационные угрозы, стоящие перед страной и обществом:

−ряд западных стран наращивает возможности информационно-технического воздействия на информационную инфраструктуру в военных целях;

−усиливается деятельность организаций, осуществляющих техническую разведку в России;

−спецслужбы отдельных государств пытаются дестабилизировать внутриполитическую и социальную ситуацию в различных регионах мира. Цель – подрыв суверенитета и нарушение территориальной целостности государств. Методы – использование информационных технологий, а также религиозных, этнических и правозащитных организаций.

−в зарубежных СМИ растет объем материалов, содержащих предвзятую оценку государственной политики России;

−российским журналистам за рубежом создаются препятствия, российские СМИ подвергаются «откровенной дискриминации»;

−террористические и экстремистские группировки нагнетают межнациональную и социальную напряженность, занимаются пропагандой, привлекают новых сторонников;

−возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере;

−растет число преступлений, связанных с нарушением конституционных прав и свобод человека, неприкосновенности частной жизни, защиты персональных данных;

−иностранные государства усиливают разведывательную деятельность в России. Растет количество компьютерных атак на объекты критической информационной инфраструктуры, их масштабы и сложность растут;

−высокий уровень зависимости отечественной промышленности от зарубежных информационных технологий (электронная компонентная ба-за, программное обеспечение, вычислительная техника, средства связи);

−низкий уровень эффективности российских научных исследований, направленных на создание перспективных информационных технологий. Отечественные разработки плохо внедряются, кадровый потенциал в этой области низкий;

−отдельные государства используют технологическое превосходство для доминирования в информационном пространстве. Управление интернетом на принципах справедливости и доверия между разными странами невозможно.

Документ называет основной стратегической целью обеспечения информационной безопасности в области обороны страны «защиту 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 госу-

дарств и представляющих угрозу международному миру, безопасности и стратегической стабильности».

Стратегия национальной безопасности Российской Федерации, утверждена Указом Президента Российской Федерации 2.07.2021 г. №400.

В разделе IV, подраздел Информационная безопасность, дается анализ угроз в области информационной безопасности РФ:

−Быстрое развитие информационно-коммуникационных технологий сопровождается повышением вероятности возникновения угроз безопасности граждан, общества и государства.

−Расширяется использование информационно-коммуникационных технологий для вмешательства во внутренние дела государств, подрыва их суверенитета и нарушения территориальной целостности, что представляет угрозу международному миру и безопасности.

−Увеличивается количество компьютерных атак на российские информационные ресурсы. Большая часть таких атак осуществляется с территорий иностранных государств.

−Активизируется деятельность специальных служб иностранных государств по проведению разведывательных и иных операций в российском информационном пространстве.

−В целях дестабилизации общественно-политической ситуации в Российской Федерации распространяется недостоверная информация, в том числе заведомо ложные сообщения об угрозе совершения террористических актов. В информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет») размещаются материалы террористических и экстремистских организаций, призывы к массовым беспорядкам. Основным объектом такого деструктивного воздействия является молодежь.

−Стремление транснациональных корпораций закрепить свое монопольное положение в сети «Интернет» и контролировать все информационные ресурсы сопровождается введением такими корпорациями (при отсутствии законных оснований и вопреки нормам международного права) цензуры и блокировкой альтернативных интернет-платформ.

−Анонимность, которая обеспечивается за счет использования информационно-коммуникационных технологий, облегчает совершение преступлений, расширяет возможности для легализации доходов, полученных преступным путем, и финансирования терроризма, распространения наркотических средств и психотропных веществ.

−Использование в Российской Федерации иностранных информационных технологий и телекоммуникационного оборудования повышает уязвимость российских информационных ресурсов к воздействию из-за рубежа.

Целью обеспечения информационной безопасности является укрепление суверенитета Российской Федерации в информационном пространстве.

Указывается, какие задачи необходимо решить для достижения цели обеспечения информационной безопасности.

Федеральный закон от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»

149-ФЗ – главный закон об информации в России. Он определяет ключевые термины, например, говорит, что информация – это любые данные, сведения и сообщения, представляемые в любой форме. Также там описано, что такое сайт, электронное сообщение и поисковая система. Именно на этот закон и эти определения нужно ссылаться при составлении документов по информационной безопасности.

В 149-ФЗ сказано, какая информация считается конфиденциальной, а какая – общедоступной, когда и как можно ограничивать доступ к информации, как происходит обмен данными. Также именно здесь прописаны основные требования к защите информации и ответственность за нарушения при работе с ней.

Ключевые моменты закона об информационной безопасности:

Нельзя собирать и распространять информацию о жизни человека без его согласия.

Все информационные технологии равнозначны – нельзя обязать компанию использовать какие-то конкретные технологии для создания информационной системы.

Есть информация, к которой нельзя ограничивать доступ, например, сведения о состоянии окружающей среды.

Некоторую информацию распространять запрещено, например, ту, которая пропагандирует насилие или нетерпимость.

Тот, кто хранит информацию, обязан ее защищать, например, предотвращать доступ к ней третьих лиц.

У государства есть реестр запрещенных сайтов. Роскомнадзор может вносить туда сайты, на которых хранится информация, запрещенная к распространению на территории РФ.

Владелец заблокированного сайта может удалить незаконную информацию и сообщить об этом в Роскомнадзор – тогда его сайт разблокируют.

Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».

Этот закон регулирует работу с персональными данными – личными данными конкретных людей. Его обязаны соблюдать те, кто собирает и хранит эти данные. Например, компании, которые ведут базу клиентов или сотрудников.

Ключевые моменты закона:

Перед сбором и обработкой персональных данных нужно спрашивать согласие их владельца.

Для защиты информации закон обязывает собирать персональные данные только с конкретной целью.

Если вы собираете персональные данные, то обязаны держать их в секрете и защищать от посторонних.

Если владелец персональных данных потребует их удалить, вы обязаны сразу же это сделать.

Если вы работаете с персональными данными, то обязаны хранить и обрабатывать их в базах на территории Российской Федерации. При этом данные можно передавать за границу при соблюдении определенных условий, прописанных в законе – жесткого запрета на трансграничную передачу данных нет.

Федеральный закон от 21.07.1993 г. № 5485-1-ФЗ «О государственной тайне»

Закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности РФ.

Положения Закона обязательны для исполнения на территории РФ и за ее пределами органами представительной, исполнительной и судебной властей, МСУ, предприятиями, учреждениями и организациями независимо от их организационно-правовой формы и формы собственности, должностными лицами и гражданами РФ, взявшими на себя обязательства либо обязанными по своему статусу исполнять требования законодательства РФ о государственной тайне.

Под ***государственной тайной*** понимаются защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ.

Определены полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты. Самостоятельный раздел Закона закрепляет перечень сведений, которые могут быть отнесены к государственной тайне.

Засекречивание сведений и их носителей – это введение для сведений, составляющих государственную тайну, ограничений на их распространение и на доступ к их носителям. Оно осуществляется в соответствии с принципами законности, обоснованности и своевременности. Определены сведения, не подлежащие засекречиванию (о чрезвычайных происшествиях и катастрофах, о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, преступности и др.).

Устанавливаются три степени секретности и соответствующие этим степеням грифы секретности для носителей сведений: «особой важности», «совершенно секретно» и «секретно».

Отнесение сведений к государственной тайне осуществляется в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью руководителями органов государственной власти в соответствии с Перечнем должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне, утверждаемым Президентом РФ. Для осуществления единой государственной политики в области засекречивания сведений межведомственная комиссия по защите государственной тайны формирует Перечень сведений, отнесенных к государственной тайне.

Рассмотрены вопросы ограничения прав собственности предприятий, учреждений, организаций и граждан РФ на информацию в связи с ее засекречиванием, порядка засекречивания сведений и их носителей, реквизитов носителей сведений, составляющих государственную тайну.

Законом регламентирован и порядок рассекречивания сведений и их носителей – снятия ранее введенных ограничений на распространение сведений, составляющих государственную тайну, и на доступ к их носителям. Основаниями для рассекречивания сведений являются: взятие на себя РФ международных обязательств по открытому обмену сведениями, составляющими в РФ государственную тайну; изменение объективных обстоятельств, вследствие которого дальнейшая защита сведений, составляющих государственную тайну, является нецелесообразной. Закреплены положения о распоряжения сведениями, составляющими государственную тайну.

Определены органы защиты государственной тайны. Допуск должностных лиц и граждан РФ к государственной тайне осуществляется в добровольном порядке. Допуск лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне осуществляется в порядке, устанавливаемом Правительством РФ.

Устанавливается три формы допуска к государственной тайне: к сведениям особой важности, совершенно секретным или секретным. Наличие у должностных лиц и граждан допуска к сведениям более высокой степени секретности является основанием для доступа их к сведениям более низкой степени секретности.

Определены основания для отказа в допуске к государственной тайне, условия прекращения допуска. Рассмотрены вопросы ограничения прав лиц, допущенных или ранее

допускавшихся к государственной тайне, организации доступа к таким сведениям и ответственности за нарушение законодательства о государственной тайне.

Средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности. Координация работ по организации сертификации средств защиты информации возлагается на межведомственную комиссию по защите государственной тайны.

За обеспечением защиты государственной тайны предусмотрены парламентский, межведомственный и ведомственный контроль, а также прокурорский надзор.

Федеральный закон от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне»

Федеральным законом регулируются отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности и предупреждением недобросовестной конкуренции. Действие Закона распространяется на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована.

Под ***коммерческой тайной*** понимается конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Устанавливается законодательное ограничение на отнесение информации к коммерческой тайне в интересах общества, государства и граждан. Так, режим коммерческой тайны ***не может быть*** установлен лицами, осуществляющими предпринимательскую деятельность, в отношении сведений о численности, составе работников, системе оплаты труда, об условиях труда, показателях производственного травматизма и профессиональной заболеваемости, наличии свободных рабочих мест, а также задолженности работодателей по выплате заработной платы и по иным социальным выплатам.

Также устанавливается обязательность предоставления на безвозмездной основе органам государственной власти и местного самоуправления по их мотивированному требованию информации, составляющей коммерческую тайну.

Законом определяются права обладателя коммерческой тайны, регулируются отношения, связанные с коммерческой тайной, полученной при выполнении государственного контракта для государственных нужд. Также устанавливаются требования к охране конфиденциальности информации, составляющей коммерческую тайну, в том числе при трудовых отношениях и в гражданско-правовых отношениях.

Предусматривается ответственность за нарушение законодательства РФ о коммерческой тайне.

Грифы, нанесенные до вступления в силу Закона на материальные носители и указывающие на содержание в них информации, составляющей коммерческую тайну, сохраняют свое действие при условии, если меры по охране конфиденциальности указанной информации будут приведены в соответствие с требованиями Закона.

Федеральный закон от 6.04.2011 г. № 63-ФЗ «Об электронной подписи»

Он расширяет сферу использования и допустимые виды электронных подписей (ЭП). Напомним, что прежний закон разрешал применять только сертифицированные средства ЭП, а область ее использования ограничивалась гражданско-правовыми отношениями.

В новой редакции выделяются ***2 вида ЭП: простая и усиленная***. Последняя может быть ***квалифицированной*** либо ***неквалифицированной***.

Простая ЭП подтверждает, что данное электронное сообщение отправлено конкретным лицом. Усиленная неквалифицированная ЭП позволяет не только однозначно идентифицировать отправителя, но и подтвердить, что с момента подписания документа его никто не изменял.

Сообщение с простой или неквалифицированной ЭП может быть приравнено к бумажному документу, подписанному собственноручно, если стороны заранее об этом договорились, а также в специально предусмотренных законом случаях.

Усиленная квалифицированная ЭП дополнительно подтверждается сертификатом, выданным аккредитованным удостоверяющим центром. Сообщение с такой ЭП во всех случаях приравнивается к бумажному документу с собственноручной подписью.

Уполномоченный в сфере ЭП орган определяет Правительство РФ. Он проводит аккредитацию удостоверяющих центров.

Закреплены требования к удостоверяющему центру. Так, стоимость его чистых активов должна составлять не менее 1 млн руб. Еще одно условие – наличие в штате квалифицированных сотрудников.

Максимальный срок аккредитации – 5 лет.

Предусмотрены механизмы признания иностранных ЭП.

Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Он регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Определены основные принципы обеспечения безопасности, полномочия госорганов, а также права, обязанности и ответственность лиц, владеющих на праве собственности или ином законном основании объектами инфраструктуры, операторов связи и информационных систем, обеспечивающих взаимодействие этих объектов.

К объектам инфраструктуры отнесены информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

Закреплены понятия компьютерной атаки, компьютерного инцидента и др. Определен порядок функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы.

Предусмотрены категорирование объектов; ведение реестра значимых объектов; оценка состояния защищенности; госконтроль; создание специальных систем безопасности.