**Часть 1. Нормализация**

Базовыми принципами развития отрасли информационных технологий на 2014 - 2020 годы и перспективу до 2025 года являются:

* улучшение институциональных условий при минимальном прямом регулировании;
* сохранение конкурентного характера развития отрасли;
* поддержка малого бизнеса в качестве приоритетного направления развития отрасли;
* определение приоритетов государственной поддержки среднего и крупного бизнеса на основе создаваемых компаниями высококвалифицированных рабочих мест, добавленной стоимости и потенциала глобальной конкурентоспособности компаний;
* обеспечение сбалансированной структуры российской отрасли, включающей крупные, средние и малые компании;
* сохранение интегрированности российской отрасли в глобальную индустрию информационных технологий;
* стимулирование капитализации компаний в России;
* стимулирование создания научно-технологического задела и новой высокотехнологичной продукции по перспективным направлениями развития отрасли;
* ориентация на государственно-частное партнерство при решении задач по развитию отрасли информационных технологий.

Правительство Российской Федерации ставит перед собой на 2014 - 2020 годы и на перспективу до 2025 года следующие основные цели развития отрасли информационных технологий:

* развитие сферы информационных технологий до полноценной отрасли российской экономики, создающей высокопроизводительные рабочие места и обеспечивающей выпуск высокотехнологичной и конкурентоспособной продукции;
* обеспечение различных сфер экономики качественными информационными технологиями с целью повышения производительности труда;
* обеспечение высокого уровня информационной безопасности государства, индустрии и граждан.

Основными задачами по развитию отрасли информационных технологий России являются:

* развитие человеческого капитала, в том числе за счет развития профильного образования и популяризации профессий отрасли;
* улучшение институциональных условий для работы компаний в России и снижение административных барьеров;
* поддержка экспорта и стимулирование глобализации отрасли;
* развитие в России исследований в сфере информационных технологий и смежных областях;
* развитие механизмов поддержки малого бизнеса, включая акселераторы, бизнес-инкубаторы, технопарки и институты, необходимые для улучшения инвестиционного климата;
* повышение грамотности населения в области информационных технологий;
* нормализация статистического наблюдения в отрасли;
* совершенствование взаимодействия органов власти, определяющих государственную политику в области информационных технологий, с отраслевыми ассоциациями, кластерами, платформами и другими объединениями;
* создание условий для развития глобальных лидеров в сфере информационных технологий в целях устранения диспропорций развития отрасли и формирования дополнительных возможностей для выкупа долей в уставном капитале компаний отрасли информационных технологий российскими инвесторами путем расширения пула крупных компаний отрасли информационных технологий в России за счет рыночных механизмов;
* дальнейшая глубокая информатизация важнейших отраслей экономики России, в том числе государственного сектора;
* стимулирование развития производства отечественной продукции посредством заказа государства и компаний с государственным участием;
* обеспечение информационной безопасности;
* широкомасштабное открытие государственных баз данных;
* развитие инфраструктуры электронной коммерции;
* развитие электронного документооборота;
* развитие центров обработки и хранения информации;
* развитие широкополосного доступа в сеть "Интернет".

Основные направления реализации Стратегии

1. Развитие кадрового потенциала и образования отрасли информационных технологий
2. Стимулирование работы высококвалифицированных специалистов отрасли информационных технологий в России
3. Популяризация информационных технологий как сферы деятельности
4. Улучшение институциональных условий развития отрасли информационных технологий
5. Международное сотрудничество и поддержка экспорта
6. Исследовательская деятельность в области информационных технологий
7. Приоритетные направления исследований и разработок в области информационных технологий
8. Поддержка развития малого бизнеса
9. Стимулирование появления лидеров отрасли информационных технологий мирового масштаба
10. Информатизация экономики и долгосрочный заказ на информационные технологии со стороны государства
11. Обеспечение информационной безопасности
12. Повышение грамотности населения в области информационных технологий
13. Статистическое обеспечение и актуализация классификаторов отрасли информационных технологий

**Часть 2. Законы**

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.

{Статья 3. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установление ограничений доступа к информации только федеральными законами;

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

6) достоверность информации и своевременность ее предоставления;

7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Статья 4. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации

1. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации основывается на Конституции Российской Федерации, международных договорах Российской Федерации и состоит из настоящего Федерального закона и других регулирующих отношения по использованию информации федеральных законов.

2. Правовое регулирование отношений, связанных с организацией и деятельностью средств массовой информации, осуществляется в соответствии с законодательством Российской Федерации о средствах массовой информации.

3. Порядок хранения и использования включенной в состав архивных фондов документированной информации устанавливается законодательством об архивном деле в Российской Федерации.}

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. Мы подробно рассматривали этот закон в отдельной статье «Как выполнить 152-ФЗ о защите персональных данных и что с вами будет, если его не соблюдать»

Ключевые моменты закона:

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

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

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

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

5. 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.

98-ФЗ «О коммерческой тайне»

Этот закон определяет, что такое коммерческая тайна, как ее охранять и что будет, если передать ее посторонним. В нем сказано, что коммерческой тайной считается информация, которая помогает компании увеличить доходы, избежать расходов или получить любую коммерческую выгоду.

Ключевые моменты закона о защите информации компании:

1. Обладатель информации сам решает, является она коммерческой тайной или нет. Для этого он составляет документ — перечень информации, составляющей коммерческую тайну.

2. Некоторые сведения нельзя причислять к коммерческой тайне, например, информацию об учредителе фирмы или численности работников.

3. Государство может затребовать у компании коммерческую тайну по веской причине, например, если есть подозрение, что компания нарушает закон. Компания обязана предоставить эту информацию.

4. Компания обязана защищать свою коммерческую тайну и вести учет лиц, которым доступна эта информация.

5. Если кто-то разглашает коммерческую тайну, его можно уволить, назначить штраф или привлечь к уголовной ответственности.

63-ФЗ «Об электронной подписи»

Этот закон касается электронной подписи — цифрового аналога физической подписи, который помогает подтвердить подлинность информации и избежать ее искажения и подделки. Закон определяет, что такое электронная подпись, какую юридическую силу она имеет и в каких сферах ее можно использовать.

Ключевые моменты закона:

1) Для создания электронной подписи можно использовать любые программы и технические средства, которые обеспечивают надежность подписи. Вы не обязаны использовать для этого какое-то конкретное государственное ПО.

2) Подписи бывают простые, усиленные неквалифицированные и усиленные квалифицированные. У них разные технические особенности, разные сферы применения и разный юридический вес. Самые надежные — усиленные квалифицированные подписи, они полностью аналогичны физической подписи на документе.

3) Те, кто работает с квалифицированной подписью, обязаны держать в тайне ключ подписи.

4) Выдавать электронные подписи и сертификаты, подтверждающие их действительность, может только специальный удостоверяющий центр.

187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Этот закон касается компаний, которые работают в сферах, критически важных для жизни государства — таких, что сбой в их работе отразится на здоровье, безопасности и комфорте граждан России.

К таким сферам относится здравоохранение, наука, транспорт, связь, энергетика, банки, топливная промышленность, атомная энергетика, оборонная промышленность, ракетно-космическая промышленность, горнодобывающая промышленность, металлургическая промышленность и химическая промышленность. Также сюда относят компании, которые обеспечивают работу предприятий из этих сфер, например, предоставляют оборудование в аренду или разрабатывают для них ПО.

Если на предприятии из этой сферы будет простой, это негативно отразится на жизни всего государства. Поэтому к IT-инфраструктуре и безопасности информационных систем на этих предприятиях предъявляют особые требования.

Ключевые моменты закона об информационной безопасности критически важных структур:

* 1. Для защиты критической инфраструктуры существует Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).
  2. Объекты критически важной инфраструктуры обязаны подключиться к ГосСОПКА. Для этого нужно купить и установить специальное ПО, которое будет следить за безопасностью инфраструктуры компании.
  3. Одна из мер предупреждения — проверка и сертификация оборудования, ПО и всей инфраструктуры, которая используется на критически важных предприятиях.
  4. Субъекты критической информационной инфраструктуры обязаны сообщать об инцидентах в своих информационных системах и выполнять требования государственных служащих. Например, использовать только сертифицированное ПО.
  5. Все IT-системы критически важных предприятий должны быть защищены от неправомерного доступа и непрерывно взаимодействовать с ГосСОПКА.
  6. При разработке IT-инфраструктуры критически важные предприятия должны руководствоваться 239 приказом ФСТЭК. В нем прописаны основные требования к защите информации на таких предприятиях.
  7. Государство имеет право проверять объекты критически важной инфраструктуры, в том числе внепланово, например, после компьютерных инцидентов вроде взлома или потери информации.

**Часть 3. Развитие IT-персонала**

Как настроить эксперта на обучение новым компетенциям

* Важно не сравнивать настоящий и предшествующий опыт, а направлять все усилия на освоение новых технологий и повышение уровня своих компетенций. Это поможет значительно ускорить процесс адаптации.
* Стоит использовать максимум возможностей для освоения нового. Получить необходимые знания можно за счет баз знаний вендоров или в аттестованных учебных центрах, которые подготавливают специальные курсы, одобренные производителем, по обучению и адаптации к работе с российским ПО. Помимо этого, существуют различные онлайн форумы и профессиональные сообщества, где специалисты могут обмениваться важными знаниями и “прокачивать” свои компетенции.
* Необходимо стремиться к расширению своих профессиональных навыков, чтобы в условиях экономических изменений оставаться востребованным на рынке труда даже при жесткой конкуренции. Самообразование и саморазвитие помогут повысить шансы оставаться “в рынке”.
* Улучшить результаты обучения, кроме профессиональных навыков, поможет “прокачка” компетенций личного развития или soft skills.

Это комплекс навыков, тесно связанных с личностными качествами, которые играют важную роль в любой профессии. Среди работодателей особо ценятся такие навыки как: коммуникабельность, умение работать в команде, способность управлять проектами, адаптивность, целеустремленность. Само собой, не лишними будут и такие качества, как ответственность, исполнительность и работоспособность.

Как освоить новые компетенции на рынке IT

С 2020 года в России стало доступно обучение по различным программам проекта «Цифровые профессии», в рамках которого государство оплачивает половину стоимости курсов. Благодаря проекту, специалисты различного уровня компетенций могут получить дополнительное образование в сфере IT.

Помимо этого, многие работодатели организуют мероприятия для повышения квалификации своих сотрудников бесплатно. Доступны также варианты обучения от российских вендоров или со стороны интеграторов, если организация использует их услуги для внедрения российского ПО. Например, в Учебном Центре Softline проводятся курсы профессиональной переподготовки и повышения квалификации для IT-специалистов, которые помогут “прокачать” компетенции или приобрести новые. В программу входит обучение взаимодействию с различными дистрибутивами ОС Linux, а по итогу выдается диплом о профессиональной переподготовке.