ЧАСТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «СЕВЕРО-КАВКАЗСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

ЛЕКЦИЯ 3. ТЕМА 1.2. ВИДЫ ПРОФЕССИОНАЛЬНОЙ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ ЧЕЛОВЕКА С ИСПОЛЬЗОВАНИЕМ ТЕХНИЧЕСКИХ СРЕДСТВ И ИНФОРМАЦИОННЫХ РЕСУРСОВ (В СООТВЕТСТВИИ С ТЕХНИЧЕСКИМ НАПРАВЛЕНИЕМ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

1. Понятие и сущность профессиональной информационной деятельности

Профессиональная информационная деятельность представляет собой трудовую деятельность, содержание которой составляют процессы сбора, обработки, хранения, передачи, производства и распространения информации, осуществляемые на профессиональной основе с применением технических средств и информационных ресурсов. Информационные технологии при этом определяются как процессы, методы поиска, сбора, хранения, обработки, предоставления и распространения информации, а также способы осуществления таких процессов и методов.

Информация в зависимости от категории доступа подразделяется на общедоступную и на информацию ограниченного доступа (в том числе профессиональную тайну — сведения, полученные лицом при исполнении профессиональных обязанностей, конфиденциальность которых возложена на него федеральным законом). Данная классификация имеет непосредственное значение для профессиональной деятельности: категория доступа определяет правовой режим работы с информацией, требования к техническим средствам её обработки и мерам ответственности за нарушение режима.

2. Виды профессиональной информационной деятельности по техническим направлениям

Применительно к техническому направлению профессиональной деятельности выделяются следующие виды информационной деятельности:

2.1. Проектирование, разработка и сопровождение информационных систем. Деятельность специалистов в области программной инженерии, включающая разработку программного обеспечения, администрирование информационных систем, проектирование баз данных и их инфраструктуры. Профессиональным продуктом здесь выступают программы для ЭВМ и базы данных, правовой режим которых регулируется частью четвёртой Гражданского кодекса Российской Федерации как объектов интеллектуальной собственности.

2.2. Эксплуатация средств вычислительной техники и информационно-телекоммуникационных сетей. Системное администрирование, обеспечение отказоустойчивости вычислительных комплексов, поддержание работоспособности каналов связи. Правила эксплуатации средств хранения, обработки и передачи компьютерной информации имеют нормативное закрепление и нарушение их влечёт юридическую ответственность.

2.3. Информационная безопасность. Деятельность по защите информации ограниченного доступа, обеспечению безопасности критической информационной инфраструктуры, внедрению организационных и программно-технических мер защиты. Данное направление регламентируется законодательством о защите информации, о государственной тайне, о персональных данных.

2.4. Управленческо-экономическая информационная деятельность. Использование информационных ресурсов для подготовки управленческих решений: работа с базами данных, электронным документооборотом, системами бизнес-аналитики.

2.5. Научно-техническая информационная деятельность. Формирование и обработка научно-технической информации: документация, патенты, лицензии, ноу-хау.

2.6. Массово-информационная деятельность. Работа средств массовой информации, коммуникационные операции с использованием телевидения, радио, телекоммуникаций и компьютерных сетей.

Общим основанием данных видов является опора на информационные ресурсы, определяемые в действующем законодательстве как отдельные документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных).

3. Стоимостные характеристики информационной деятельности

Информация рассматривается как экономический ресурс, обладающий особыми свойствами: она не расходуется при потреблении, способна к многократному использованию, а информационные ресурсы растут тем быстрее, чем интенсивнее их используют. Стоимость информации как товара определяется трудом, вложенным в её производство; при этом информация снижает неопределённость экономических решений, влияет на поведение хозяйствующих субъектов и сама может обладать рыночной стоимостью.

Информационный продукт — результат деятельности человека, представленный на материальном носителе; информационная услуга — получение и предоставление в распоряжение пользователя информационного продукта. Экономическую эффективность информационной деятельности определяют с помощью трудовых и стоимостных показателей.

Под прямой экономической эффективностью информационных технологий понимается экономия материально-трудовых ресурсов и денежных средств, полученная в результате автоматизации информационных работ: сокращения численности персонала, уменьшения фонда заработной платы, расхода основных и вспомогательных материалов.

Основные стоимостные показатели рассчитываются сопоставлением затрат на обработку информации при базисном (C_0) и отчётном (C_1) вариантах:

- абсолютный показатель экономии стоимости:

$$C_{\text{эк}} = C_0 - C_1;$$

- индекс стоимости затрат:

$$J_{\text{ст.зат}} = \frac{C_1}{C_0};$$

- срок окупаемости затрат на создание проекта:

$$T_{\text{ок}} = \frac{K_N}{C_{\text{эк}}},$$

где K_N — совокупные затраты на создание проекта (лицензии на программное обеспечение, стоимость оборудования, премиальный фонд участников проекта).

Наряду с прямыми показателями учитывается косвенная экономическая эффективность: повышение качества управленческих решений, сокращение времени поиска информации, снижение риска финансовых потерь. Поскольку ценность информации состоит в возможности предоставить потребителю дополнительную свободу действий, стоимостная оценка информационной деятельности носит двойственный характер: она включает как затраты на производство и обработку информации, так и приносимый ею экономический эффект.

4. Правовые нормы, относящиеся к информации

Правовое регулирование информационной сферы в Российской Федерации базируется на Конституции РФ (ст. 23, 24, 29) и представлено иерархически организованной системой нормативных актов.

4.1. Базовый уровень. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» устанавливает понятийный аппарат, классификацию информации по категориям доступа и порядку распространения, принципы правового регулирования, требования к созданию и эксплуатации информационных систем.

4.2. Персональные данные. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» определяет правовой статус оператора и субъекта персональных данных, устанавливает принципы обработки (законность, целевое ограничение, минимизация, конфиденциальность) и обязанности оператора по обеспечению безопасности данных при их обработке.

4.3. Гражданско-правовой блок. Часть четвёртая ГК РФ регулирует отношения по поводу объектов интеллектуальной собственности: программ для ЭВМ, баз данных, произведений науки, литературы и искусства, промышленной собственности.

4.4. Уголовно-правовой блок. Глава 28 УК РФ «Преступления в сфере компьютерной информации» охватывает широкий круг составов:

ст. 272 — неправомерный доступ к охраняемой законом компьютерной информации, повлёкший уничтожение, блокирование, модификацию либо копирование информации; квалифицирующими признаками выступают крупный ущерб, корыстная заинтересованность, использование служебного положения, групповой характер деяния, тяжкие последствия (лишение свободы до десяти лет);

- ст. 272.1 — незаконные использование, передача, сбор и хранение компьютерной информации, содержащей персональные данные, полученной незаконным путём;
- ст. 273 — создание, использование и распространение вредоносных компьютерных программ (до семи лет лишения свободы при тяжких последствиях);
- ст. 274 — нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, повлёкшее крупный ущерб;
- ст. 274.1 — неправомерное воздействие на критическую информационную инфраструктуру РФ;
- ст. 274.2–274.6 — нарушение правил централизованного управления техническими средствами противодействия угрозам в сети «Интернет», незаконное использование абонентского терминала пропуска трафика, неправомерная организация передачи абонентских номеров и данных авторизации пользователей.

Смежные составы содержатся в главе 23 УК РФ (ст. 183 — незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну), а также в статьях об ответственности за нарушения авторских и смежных прав (ст. 146).

4.5. Административно-правовой блок. Статья 13.11 КоАП РФ устанавливает ответственность за нарушения законодательства о персональных данных. После вступления в силу изменений, предусмотренных Федеральным законом от 30.11.2024 № 420-ФЗ, санкции существенно ужесточены:

- обработка персональных данных вне требований законодательства — штраф для организаций от 150 000 до 300 000 руб. (при повторном нарушении — от 300 000 до 500 000 руб.);
- неуведомление Роскомнадзора о начале обработки персональных данных — для организаций до 300 000 руб.;
- неуведомление об инциденте утечки — до 3 млн руб. для организаций;

• неправомерная передача данных от 1 000 до 10 000 субъектов — для организаций от 3 до 5 млн руб.; от 10 000 до 100 000 субъектов — от 5 до 10 млн руб.; свыше 100 000 субъектов — от 10 до 15 млн руб.;

• утечка данных специальной категории — до 15 млн руб.; утечка биометрических персональных данных — от 15 до 20 млн руб.;

• за повторные крупные утечки предусмотрены оборотные штрафы: от 1 до 3 % годовой выручки организации, но не менее 20 млн руб. и не более 500 млн руб.. it-pnk.ru +1

5. Правонарушения в информационной сфере

По субъектно-объектному составу правонарушения в информационной сфере целесообразно классифицировать следующим образом:

5.1. Нарушения режима доступа к информации. Неправомерный доступ, несанкционированное копирование, уничтожение и модификация информации; нарушение правил эксплуатации средств её обработки.

5.2. Нарушения режима распространения информации. Распространение запрещённой информации, диффамация, нарушение тайны связи и профессиональной тайны.

5.3. Нарушения прав на объекты интеллектуальной собственности. Пиратское использование программного обеспечения, контрафакция, нарушение авторских и смежных прав, патентных прав.

5.4. Нарушения при обработке персональных данных. Обработка без правового основания, нарушение принципов минимизации и целевого ограничения, утечки данных по вине оператора, необеспечение безопасности информационных систем персональных данных.

5.5. Преступления против информационной инфраструктуры. Распространение вредоносных программ, атаки на критическую информационную инфраструктуру, злоупотребление средствами авторизации и передачи номеров.

Существенно, что статистика судебной практики 2019–2024 годов демонстрирует устойчивый рост числа приговоров по ст. 272 УК РФ и особенно по ст. 274.1 УК РФ (количество приговоров по массовой части последней выросло по сравнению с 2019 годом в шестнадцать раз), что отражает усиление уголовно-правовой охраны информационной сферы.

6. Меры предупреждения правонарушений в информационной сфере

Система предупреждения правонарушений в информационной сфере строится по трём уровням.

Правовой уровень включает: актуализацию внутренних регламентов с учётом действующих редакций 149-ФЗ и 152-ФЗ; документирование правовых оснований обработки информации (согласия субъектов, поручения, договоры); установление режима профессиональной тайны с подписанием соглашений о конфиденциальности. С 1 сентября 2025 года законодательство о персональных данных ужесточило требования к уведомлению Роскомнадзора и порядку трансграничной передачи данных, что делает регулярный правовой аудит обязательным элементом деятельности оператора.

Организационный уровень предусматривает: разграничение прав доступа по принципу минимальной достаточности; назначение лиц, ответственных за организацию обработки персональных данных в организации; проведение обучения персонала по вопросам информационной безопасности; регламентацию реагирования на инциденты, включая обязанность уведомления Роскомнадзора об утечке персональных данных.

Технический уровень охватывает: применение сертифицированных средств защиты информации; многофакторную аутентификацию; резервное копирование и журналирование операций; средства мониторинга неправомерного доступа. Соблюдение правил эксплуатации средств хранения, обработки и передачи компьютерной информации

имеет не только инженерное, но и правовое значение, поскольку их нарушение при крупном ущербе образует состав преступления (ст. 274 УК РФ).

Выводы

Профессиональная информационная деятельность в технической сфере представляет собой многоуровневую систему видов труда — от разработки информационных систем до обеспечения их безопасности, — экономика которой описывается трудовыми и стоимостными показателями (экономия затрат, индекс стоимости, срок окупаемости). Правовой режим этой деятельности определяется Конституцией РФ, федеральными законами № 149-ФЗ и № 152-ФЗ, частью четвёртой ГК РФ, а ответственность за правонарушения — нормами главы 28 УК РФ и ст. 13.11 КоАП РФ с существенно возросшими санкциями за утечки персональных данных. Предупреждение правонарушений достигается сочетанием правового, организационного и технического уровней обеспечения информационной безопасности.