**Законодательные акты по легализации и защите компьютерной информации**

Для полноценной и своевременной защиты государства и общества от угроз необходимо постоянно модернизировать существующее законодательство. Процесс всемирной информатизации и компьютеризации привел к тому, что повсеместное широкое внедрение в повседневную жизнь информационных технологий повлекло появление новых вызовов и угроз. В это же время мировое сообщество столкнулось с понятием киберпреступления. В связи с этим во многих странах мира формируется законодательство, регулирующее отношения в сфере компьютерной информации. В России в январе 1997 года был принят новый Уголовный кодекс Российской Федерации, в который была включена глава 28 «Преступления в сфере компьютерной информации» в составе трёх статей:

 статья 272 «Неправомерный доступ к компьютерной информации»;

- статья 273 «Создание, использование, распространение вредоносных программ для ЭВМ»;

- статья 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети».

Исходя из диспозиций приведённых статей, можно сказать, что глава 28 УК РФ имеет своей целью обеспечение информационной безопасности, и как следствие обеспечение защиты аппаратно-технических средств, являющихся [материал](https://moodle.birskdo.ru/mod/glossary/showentry.php?eid=2126&displayformat=dictionary)ьными носителями информационных ресурсов.  
В отечественном законодательстве, регулирующем отношения в сфере компьютерной информации, произошли серьёзные изменения. К таким нормативно – правовым актам, относятся:

- Федеральный закон от 27 июля 2006 года № 149 – ФЗ «Об информации, информационных технологиях и о защите информации» (в ред. Федерального закона от 27.07.2010 N 227-ФЗ);

- Федеральный закон от 27 июля 2006 года №152 – ФЗ «О персональных данных» (в ред. от 23.12.2010 N 359-ФЗ);

- Федеральный закон от 22 октября 2004 года №125 – ФЗ «Об архивном деле в Российской Федерации», где архивный документ определяется как [материал](https://moodle.birskdo.ru/mod/glossary/showentry.php?eid=2126&displayformat=dictionary)ьный носитель с зафиксированной на нем информацией, который имеет реквизиты, позволяющие его идентифицировать, и подлежит хранению в силу значимости указанных носителя и информации для граждан, общества и государства». В связи с тем, что под понятие «[материал](https://moodle.birskdo.ru/mod/glossary/showentry.php?eid=2126&displayformat=dictionary)ьный носитель» попадает понятие «машинный носитель информации», отношения в сфере архивного дела также регулируются основными нормативно – правовыми актами в сфере компьютерной информации.

Кроме того, в связи с новоявленными угрозами в сфере компьютерной информации и компьютерной безопасности, были внесены дополнения и изменения в следующие нормативно-правовые документы:

- Федеральный закон от 21 июля 1993 года № 5485 – 1 «О государственной тайне» (в ред. от 18.07.2009 N 180-ФЗ);

- Федеральный закон от 29 июля 2004 года № 98 – ФЗ «О коммерческой тайне» (в ред. от 24.07.2007 N 214-ФЗ);

- Федеральный закон от 29 декабря 1994 № 77 – ФЗ «Об обязательном экземпляре документов» (в ред. от 23.07.2008 N 160-ФЗ);

- Федеральный закон от 27 декабря 1991 года №2124-1 «О средствах массовой информации» (в ред. от 09.02.2009 N 10-ФЗ) и др.

Так, целый ряд законов лишился своей юридической силы вследствие введения 18 декабря 2006 года в Гражданский кодекс Российской Федерации части четвертой, раздела шестого «Права на результаты интеллектуальной деятельности и средства индивидуализации».

Для контроля обеспечения информационной и компьютерной безопасности 7 октября 1998 года в структуре МВД РФ было создано специальное подразделение по борьбе с преступлениями в сфере высоких технологий – Управление БПСВТ. Ему был придан статус оперативно – розыскного подразделения. В 2001 году УБПСВТ было упразднено, а его штат, структура и [материал](https://moodle.birskdo.ru/mod/glossary/showentry.php?eid=2126&displayformat=dictionary)ьно – техническое обеспечение было передано Бюро специальных технических мероприятий (БСТМ) при МВД РФ и в настоящее время имеет название Управление «К» МВД РФ (Управление по борьбе с компьютерными преступлениями). Наряду с отделами «К» в структуре Главного управления по борьбе с экономическими преступлениями (ГУБЭП) МВД России в субъектах Российской Федерации с 1997 года были созданы специализированные подразделения – Отделы по борьбе с преступлениями в сфере экономики и компьютерной информации, которые осуществляют выявление, пресечение и предварительное расследование хищений, совершаемых с использованием электронных документов, мошенничеств с кредитными либо расчетными картами, а также незаконного использования объектов авторского права и смежных прав, находящихся на машинных носителях. В 1997 году в подразделениях Следственного комитета при МВД России, функционирующих при МВД, ГУВД и УВД субъектов Российской Федерации, создаются специализированные следственные отделы и отделения по расследованию преступлений в сфере экономики и компьютерной информации. Следователи органов внутренних дел, входящие в состав таких подразделений, тесно взаимодействуют со специализированными органами дознания – Отделами «К» и ОБЭП.

Таким образом, в современных исследованиях по вопросам преступлений в сфере компьютерной информации, отмечается, что в качестве объекта таких преступлений выступает информация, с ограниченным доступом, представляющая собой особую ценность, и требующая особой правовой охраны. Поэтому особую актуальность приобретают те аспекты, которые требуют отслеживания последних изменений и дополнений в современном российском законодательстве в области информационной безопасности в целом.

**Государственная политика в области защиты информационных ресурсов общества**

***Концепция государственной информационной политики 1998 г.*** призвана сыграть роль организующего и координирующего документа, представляющего основу для подготовки государственной программы по вхождению России в информационное общество. Одно из назначений Концепции – обратить внимание органов государственной власти, средств массовой информации, всех заинтересованных лиц на проблемы подготовки государства, общества, личности к условиям жизни в информационном обществе.

Согласно этой Концепции **основными задачами государственной информационной политики** являются:

* развитие информационно-телекоммуникационных технологий;
* эффективное формирование и использование национальных информационных ресурсов (ИР) и обеспечение широкого, свободного доступа к ним;
* обеспечение граждан общественно значимой информацией и развитие независимых средств массовой информации;
* подготовка человека к жизни и работе в грядущем информационном веке;
* обеспечение информационной безопасности.

Правовое обеспечение государственной информационной политики должно развиваться по следующим основным направлениям: разработка новых законов, дополняющих и развивающих существующее законодательство в информационной сфере; совершенствование актов действующего законодательства, повышение эффективности их норм; систематизация и кодификация актов информационного законодательства; согласование существующих и вновь разрабатываемых законов в информационной сфере с актами других отраслей законодательства; активное участие в разработке международного законодательства в информационной сфере (на уровне ближнего и дальнего зарубежья).

**Первоочередными мероприятиями государственной информационной политики** в области информационного права **должны быть:**

* анализ процессов развития информационной сферы, выявление пробелов и дублей в законодательстве;
* разработка концепции формирования и развития информационного права и его источника – информационного законодательства;
* анализ причин низкой эффективности существующего информационного законодательства и определение необходимого комплекса мер по исправлению этого положения;
* повышение информационно-правовой культуры общества.

**Основные положения правового обеспечения государственной информационной политики** в рамках информационного права:

* реализация принципа правового равенства всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса;
* формирование нормативной правовой базы, обеспечивающей эффективное регулирование информационных отношений, а также осуществление контроля за безусловным исполнением законодательства;
* признание возможности ограничения доступа к информации исключительно на основе закона как исключения из общего принципа открытости информации;
* персонифицирование ответственности за сохранность информации, ее засекречивание и рассекречивание;
* защита законными средствами личности, общества, государства от ложной, искаженной и недостоверной информации;
* предоставление гражданам универсальной общественной информационной услуги, способствование доступу к мировым информационным ресурсам, глобальным информационным сетям.