

## ТЕМА 2: НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

### 2.1. Общие положения

На ближайших двух лекциях мы рассмотрим ряд законодательных актов, затрагивающих вопросы информатизации, применения электронно-цифровой подписи и ответственности возникающей в случае осуществления правонарушений в сфере информационной безопасности.

Информация все в большей степени становится товаром, от наличия и сохранности которого зависит благополучие как отдельных граждан и организаций, так и общества в целом. Отсюда неизбежно возникает проблема обеспечения информационной безопасности с целью предотвращения хищения или искажения информации, блокирования процесса ее получения, противодействия попыткам внедрения ложной информации. При этом необходимо учитывать то, что информация является весьма специфическим продуктом, который может существовать в материализованном и в нематериализованном (нефиксированном) виде.

Правовая защита информации как ресурса признана на международном, государственном уровне и определяется межгосударственными договорами, конвенциями, декларациями и реализуется патентами, авторским правом и лицензиями на их защиту.

Дадим определение следующим понятиям:

- **под информационной безопасностью** понимается состояние защищенности жизненно важных интересов личности, общества и государства от внешних и внутренних угроз в сфере информационных отношений (*не в информационной сфере*).
- **под безопасностью информации** понимается такое ее состояние, при котором исключается возможность *ознакомления* с этой информацией, ее *изменения или уничтожения* лицами, не имеющими на это права, а также *утечки* за счет побочных электромагнитных излучений и наводок, специальных устройств перехвата (уничтожения) при передаче между объектами вычислительной техники.
- **под защитой информации** понимается совокупность мероприятий, направленных на обеспечение *конфиденциальности и целостности* обрабатываемой информации, а также *доступности информации* для пользователей.

Для защиты информации необходимо наличие целого комплекса правовых норм, которые определили бы правовой режим информации. В самом общем виде “правовой

режим информации” следует понимать как совокупность нормативно установленных правил, определяющих:

- права собственности, владения и распоряжения информацией;
- степень открытости информации (необходимость или возможность ее отнесения к категории ограниченного доступа);
- порядок отнесения информации к категории ограниченного доступа и перечень уполномоченных на это лиц;
- порядок документирования, доступа, хранения, контроля и распространения информации;
- нормы, регулирующие применение различных средств и методов обеспечения информационной безопасности;
- порядок привлечения к ответственности и меры наказания за нарушение установленных норм и правил в области информационных отношений.

Комплексное изучение установленных норм и правил в конкретной прикладной области является обязательным элементом правовой культуры работающего в этой области специалиста.

## **2.2. Правовое обеспечение защиты информации**

Можно выделить следующую структуру законодательства Республики Беларусь в области информатизации:

- Конституционное законодательство
- Общие законы, кодексы, которые включают нормы по вопросам информатизации и информационной безопасности
  - Банковский кодекс
  - Закон Республики Беларусь «О государственных секретах»
  - Закон Республики Беларусь «Об информатизации»
  - Закон Республики Беларусь «Об национальном архивном фонде и архивах Республики Беларусь»
  - Декрет Президента Республики Беларусь «О лицензировании отдельных видов деятельности» от 14 июля 2003 г. N 17
- Законы об организации управления
  - Закон Республики Беларусь «Об органах государственной безопасности»
  - Закон Республики Беларусь «О милиции»
- Специальные законы
  - Закон Республики Беларусь «Об электронном документе»
- Подзаконные акты
  - Положение о Государственном центре безопасности информации при Президенте Республики Беларусь
  - Положение о коммерческой тайне
  - Инструкция о ДСП
- Правоохранительное законодательство
  - Уголовный кодекс
  - Гражданский кодекс

- Кодекс об административных правонарушениях

Далее мы кратко рассмотрим некоторые законодательные акты.

### **2.3. Закон РБ О государственных секретах**

Закон РБ «О государственных секретах» определяет правовые и организационные основы отнесения сведений к государственным секретам, защиты государственных секретов, осуществления иной деятельности в сфере государственных секретов в целях обеспечения национальной безопасности Республики Беларусь.

Под государственными секретами (сведениями, составляющими государственные секреты) будем понимать сведения, отнесенные в установленном порядке к государственным секретам, защищаемые государством в соответствии с законодательством Республики Беларусь.

К государственным секретам могут быть отнесены:

- сведения в области политики:
  - о стратегии и тактике внешней политики, а также внешнеэкономической деятельности;
  - о подготовке, заключении, содержании, выполнении, приостановлении или прекращении действия международных договоров Республики Беларусь;
  - об экспорте и импорте вооружения и военной техники;
  - о содержании или объемах экономического сотрудничества с иностранными государствами в военное время;
- сведения в области экономики и финансов:
  - о содержании планов подготовки экономики к отражению возможной военной агрессии;
  - о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники;
  - о планах (заданиях) государственного оборонного заказа, об объемах выпуска и поставках вооружения и военной техники, военно-технического имущества;
  - об объемах финансирования из республиканского бюджета Вооруженных Сил Республики Беларусь, других войск и воинских формирований, правоохранительных и иных государственных органов, обеспечивающих национальную безопасность Республики Беларусь;
  - о технологии изготовления системы защиты, применяемой при производстве денежных знаков, бланков ценных бумаг и других документов с определенной степенью защиты, обеспечиваемых государством;
- сведения в области науки и техники:
  - о содержании государственных и других программ, концепций по направлениям, определяющим национальную безопасность Республики

Беларусь;

- о проведении научно-исследовательских, опытно-технологических и опытно-конструкторских работ в интересах национальной безопасности Республики Беларусь;
- сведения в военной области:
  - о планах строительства Вооруженных Сил Республики Беларусь, содержании основных направлений (программ) развития вооружения и военной техники;
  - о тактико-технических характеристиках и возможностях боевого применения вооружения и военной техники;
  - о системе управления Вооруженными Силами Республики Беларусь;
  - о содержании стратегических или оперативных планов, планов территориальной обороны, документов боевого управления по подготовке и проведению операций, стратегическому разворачиванию Вооруженных Сил Республики Беларусь, других войск и воинских формирований, их боевой, мобилизационной готовности и мобилизационных ресурсах;
  - о назначении, местонахождении, степени защищенности, системе охраны особо режимных и режимных объектов, пунктов управления государством в военное время или их проектировании, строительстве, эксплуатации, степени готовности;
- сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности:
  - об организации, тактике, силах, средствах, объектах, методах, планах разведывательной, контрразведывательной и оперативно-розыскной деятельности, в том числе по обеспечению собственной безопасности в органах, осуществляющих такую деятельность;
  - о финансировании мероприятий, проводимых органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность;
  - о гражданах, сотрудничающих (сотрудничавших) на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность, а также о штатных негласных сотрудниках и сотрудниках этих органов, в том числе внедренных в организованные группы, выполняющих (выполнявших) специальные задания;
- сведения в информационной и иных областях национальной безопасности Республики Беларусь:
  - о содержании, организации или результатах основных видов деятельности Совета Безопасности Республики Беларусь, государственных органов, обеспечивающих национальную безопасность Республики Беларусь;
  - об организации, силах, средствах и методах обеспечения безопасности охраняемых граждан и защиты охраняемых объектов;
  - о финансировании мероприятий, проводимых в целях обеспечения безопасности охраняемых граждан и защиты охраняемых объектов;
  - о системе, методах и средствах защиты государственных секретов, состоянии защиты государственных секретов;
  - о шифрах, системах шифрованной, других видов специальной связи;

- иные сведения в области политики, экономики, финансов, науки, техники, в военной области, области разведывательной, контрразведывательной, оперативно-розыскной деятельности, информационной и иных областях национальной безопасности Республики Беларусь, которые включаются в перечень сведений, подлежащих отнесению к государственным секретам.

К государственным секретам не могут быть отнесены сведения:

- являющиеся общедоступной информацией, доступ к которой, распространение и (или) предоставление которой не могут быть ограничены в соответствии с законодательными актами Республики Беларусь;
- находящиеся в собственности иностранных государств, международных организаций, межгосударственных образований и переданные Республике Беларусь.

Государственные секреты подразделяются на две категории: государственную тайну (сведения, составляющие государственную тайну) и служебную тайну (сведения, составляющие служебную тайну).

**Государственная тайна** – сведения, в результате разглашения или утраты которых могут наступить тяжкие последствия для национальной безопасности Республики Беларусь.

**Служебная тайна** – сведения, в результате разглашения или утраты которых может быть причинен существенный вред национальной безопасности Республики Беларусь.

Служебная тайна может являться составной частью государственной тайны, не раскрывая ее в целом.

Для государственных секретов в зависимости от тяжести последствий, которые наступили или могут наступить, размера вреда, который причинен или может быть причинен в результате их разглашения или утраты, устанавливаются следующие **степени секретности**:

- для государственной тайны – «Особой важности», «Совершенно секретно»;
- для служебной тайны – «Секретно».

На носителях государственных секретов и (или) сопроводительной документации к ним в зависимости от степени секретности государственных секретов проставляются **грифы секретности**:

- на носителях государственной тайны и (или) сопроводительной документации к ним – «Особой важности», «Совершенно секретно»;
- на носителях служебной тайны и (или) сопроводительной документации к ним – «Секретно».

Допуск к госсекретам связан с ограничениями прав и дополнительными

обязанностями для физических лиц. В соответствии с законодательством ограничиваются права выезда за границу, пользования и распоряжения секретными сведениями. Так, только руководитель организации, допуская к секретам, может разрешить работнику выехать за границу в период, оговоренный в договоре о допуске. Даже авторы секретных изобретений и открытий вправе распространять сведения о них только в порядке, определяемом секретным делопроизводством.

Наряду с ограничениями существуют определенные гарантии прав и интересов лиц, связанных с секретами. В первую очередь это касается защиты интеллектуальной собственности в сфере науки и технологий, обеспечении конкурентоспособности отечественных производителей на рынке наукоемкой продукции, а также права на получение более обширной информации по каким-либо вопросам или в определенной сфере деятельности, что для профессиональной деятельности многих весьма важно. Сейчас, например, ведется разработка нормативных правовых актов, которые будут регулировать вопросы защиты прав и законных интересов физических и юридических лиц в рассматриваемой сфере.

Кроме этого, законодательство предусматривает компенсации за ограничения прав носителя секретов, которые выражаются в виде доплат к должностному окладу или тарифной ставке в размерах, определяемых постановлениями Совмина, Минтруда и соцзащиты.

Допуск к государственным секретам гражданам предоставляется, если:

- граждане ознакомлены с правами и обязанностями, предусмотренными Законом «О государственных секретах» и другими актами законодательства Республики Беларусь о государственных секретах, с возможным временным ограничением их права на выезд из Республики Беларусь, а также с законодательными актами Республики Беларусь, устанавливающими ответственность за нарушение законодательства Республики Беларусь о государственных секретах;
- имеется письменное согласие граждан на проведение в отношении их проверочных мероприятий в связи с предоставлением им допуска к государственным секретам;
- гражданами представлены их персональные данные;
- гражданами приняты письменные обязательства перед государством о соблюдении законодательства Республики Беларусь о государственных секретах;
- имеется согласование уполномоченным государственным органом по защите государственных секретов предоставления им допуска к государственным секретам;
- проведены проверочные мероприятия в отношении граждан в связи с предоставлением им допуска к государственным секретам.

## 2.4. Положение о коммерческой тайне

06.11.1992 Советом Министров РБ было принято Положение о коммерческой тайне.

Данное положение определяет экономические и правовые основы защиты коммерческой тайны.

Коммерческую тайну составляют преднамеренно скрываемые экономические интересы и информация о различных сторонах и сферах производственно-хозяйственной, управленческой, научно-технической, финансовой деятельности субъекта хозяйствования, охрана которых обусловлена интересами конкуренции и возможной угрозой экономической безопасности субъекта хозяйствования.

Информация, составляющая коммерческую тайну, является собственностью субъекта хозяйствования либо находится в его владении, пользовании, распоряжении в пределах, установленных собственником и законодательными актами.

Информация, составляющая коммерческую тайну, должна соответствовать следующим требованиям:

- иметь действительную или потенциальную ценность для субъекта хозяйствования по коммерческим причинам;
- не являться общеизвестной или общедоступной согласно законодательству Республики Беларусь;
- обозначаться соответствующим образом с осуществлением субъектом хозяйствования надлежащих мер по сохранению ее конфиденциальности через систему классификации информации как коммерческой тайны, разработки внутренних правил засекречивания, введения соответствующей маркировки документов и иных носителей информации, организации секретного делопроизводства;
- не являться государственным секретом и не защищаться авторским и патентным правом;
- не касаться негативной деятельности субъекта хозяйствования, способной нанести ущерб интересам государства.

Коммерческую тайну субъекта хозяйствования не могут составлять:

- учредительные документы, а также документы, дающие право на занятие предпринимательской деятельностью и отдельными видами хозяйственной деятельности;
- сведения по установленным формам отчетности о финансово-хозяйственной деятельности и иные данные, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей;
- документы о платежеспособности;
- сведения о численности и составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест.

Содержание и объем информации, составляющей коммерческую тайну, а также порядок ее защиты определяются руководителем субъекта хозяйствования, который доводит их до работников либо лиц, имеющих доступ к таким сведениям.

Работники субъекта хозяйствования и лица, заключившие гражданско-правовые договоры, имеющие доступ к коммерческой тайне субъекта хозяйствования, принимают обязательство сохранять коммерческую тайну и без разрешения, выданного в установленном порядке, не разглашать сведения, ее составляющие, при условии, что эта информация ранее не была известна работникам или иному лицу, получившему к ней доступ, либо не была получена от третьей стороны без обязательства соблюдать в отношении ее конфиденциальность.

Данное обязательство дается в письменной форме при приеме на работу, заключении гражданско-правового договора либо в процессе его исполнения.

Указанные лица вправе передать конфиденциальную информацию третьим лицам в случае привлечения их к деятельности, требующей знания такой информации, только в том объеме, который необходим для реализации целей и задач субъекта хозяйствования.

Передача третьим лицам информации, являющейся коммерческой тайной, влечет за собой установленную законодательством ответственность при условии, что сведения содержались в тайне, что они были в установленном порядке вверены разгласившему их лицу без согласия на разглашение и что разглашением был причинен ущерб.

## **2.5. Закон РБ «Об электронном документе и электронной цифровой подписи»**

Впервые Закон об электронном документе был принят в Беларуси 10 января 2000 года.

Однако в связи с необходимостью более широкого применения электронных документов в деятельности различных субъектов хозяйствования нашей страны, а также с целью создания правовой предпосылки построения инфраструктуры открытых ключей, в декабре 2009г. был подписан новый Закон Республики Беларусь «Об электронном документе и электронной цифровой подписи».

Данный Закон устанавливает правовые основы применения электронных документов, определяет основные требования, предъявляемые к электронным документам, а также права, обязанности и ответственность участников правоотношений, возникающих в сфере обращения электронных документов.

Рассмотрим основные понятия, применяемые в данном законе:

**Электронный документ** (далее ЭД) – документ в электронном виде с реквизитами, позволяющими установить его целостность и подлинность.



Под **подлинностью** понимается свойство электронного документа, определяющее, что электронный документ подписан действительной электронной цифровой подписью (или несколькими электронными цифровыми подписями). **Целостность** ЭД - это свойство электронного документа, определяющее, что в электронный документ не были внесены изменения и (или) дополнения (например, в процессе его передачи по каналам связи).

Реквизитом, позволяющим установить подлинность и целостность ЭД является **электронная цифровая подпись** (далее ЭЦП).

Для генерации ЭЦП используются асимметричные алгоритмы. В таких алгоритмах применяется пара ключей – открытый и закрытый (личный).

**Личный ключ** электронной цифровой подписи (далее – личный ключ) – последовательность символов, принадлежащая определенной организации или физическому лицу и используемая при выработке электронной цифровой подписи.

**Открытый ключ** – последовательность символов, соответствующая определенному личному ключу, доступная для всех заинтересованных организаций или физических лиц и применяемая при проверке электронной цифровой подписи.

Необходимым условием того, чтобы электронный документ имел юридическую силу на территории Беларуси, для генерации ЭЦП необходимо использовать сертифицированные средства ЭЦП.

Под **средством ЭЦП** будем понимать программное, программно-техническое или техническое средство, с помощью которого реализуются одна или несколько из следующих функций: выработка электронной цифровой подписи, проверка электронной цифровой подписи, выработка личного ключа или открытого ключа.

При широком использовании электронных документов встает вопрос о передаче открытого ключа ЭЦП своим контрагентам, таким образом, чтобы сохранилась его целостность и подлинность.

Именно с этой целью встает вопрос о создании инфраструктуры открытых ключей (создание правил и организационно-технических способов их распространения).

Как правило, распространения открытых ключей происходит посредством сертификатов открытого ключа.

**Сертификат открытого ключа** – электронный документ, изданный поставщиком услуг и содержащий информацию, подтверждающую принадлежность указанного в нем открытого ключа определенной организации или физическому лицу, и иную информацию, предусмотренную законодательством Республики Беларусь.

Электронный документ состоит из двух неотъемлемых частей – общей и особенной.

Общая часть электронного документа состоит из информации, составляющей содержание документа.

Особенная часть электронного документа состоит из одной или нескольких электронных цифровых подписей, а также может содержать дополнительные данные, необходимые для проверки электронной цифровой подписи (электронных цифровых подписей) и идентификации электронного документа, которые устанавливаются техническими нормативными правовыми актами.

**Оригинал электронного документа** существует только в электронном виде. Все идентичные экземпляры электронного документа являются оригиналами и имеют одинаковую юридическую силу.

Документы, созданные организацией или физическим лицом на бумажном носителе и в электронном виде, идентичные по содержанию, имеют одинаковую юридическую силу. В этом случае документ на бумажном носителе не является копией электронного документа.

**Копией электронного документа** считается форма внешнего представления электронного документа на бумажном носителе, удостоверенная в порядке, установленном законодательством Республики Беларусь.

Удостоверять ЭД могут:

- нотариус или другое должностное лицо, имеющее право совершать нотариальные действия;
- организация или индивидуальный предприниматель, имеющий право на осуществление подобной деятельности.

Копия электронного документа должна содержать указание на то, что она является копией соответствующего электронного документа.

Стоит отметить, что подлинный электронный документ приравнивается к документу на бумажном носителе, подписанному собственноручно, и имеет одинаковую с ним юридическую силу.

Сегодня электронные документы широко применяются в банковских организациях Беларуси. Например, большинство документов между Национальным банком и коммерческими банками, а также между ком.банком и его клиентами идет в виде электронных документов.