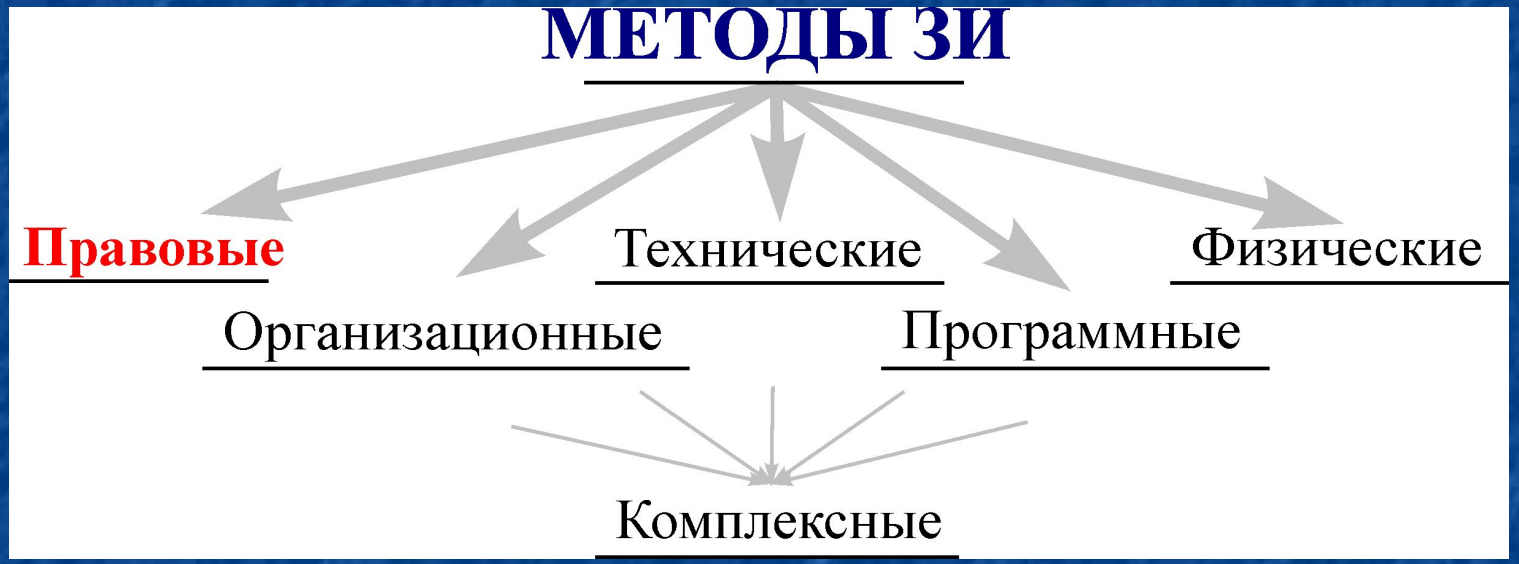
Правовые и организационные методы защиты информации

КЛАССИФИКАЦИЯ МЕТОДОВ ЗИ



Правовые методы ЗИ

Правовое обеспечение ЗИ:

Нормотворческая деятельность

Создание законодательства в области информационной безопасности

Исполнительная и правоприменительная деятельность

Контроль за исполнением законодательства государственными органами, организациями и гражданами;

Нормотворческая деятельность

- Оценка состояния действующего законодательства и разработка программы его совершенствования;
- Создание организационно-правовых механизмов обеспечения информационной безопасности;
- Формирование прав и обязанностей всех субъектов в системе информационной безопасности;
- Разработка организационно-правового механизма сбора и анализа статистических данных о воздействии угроз информационной безопасности и их последствиях;
- Разработка нормативных актов, регулирующих порядок ликвидации последствий воздействий угроз.

Исполнительная и правоприменительная деятельность:

1. Разработка процедур применения законодательства и нормативных актов к субъектам, совершившим преступления и проступки при работе с закрытой информацией;

2. Разработка составов правонарушений с учетом специфики уголовной, гражданской, административной и дисциплинарной ответственности.

Деятельность по правовому обеспечению информационной безопасности строится на трех фундаментальных положениях:

1. Соблюдение законности (предполагает наличие законов и иных нормативных документов, их применение и исполнение субъектами права в области информационной безопасности);
2. Обеспечение баланса интересов отдельных субъектов и государства (предусматривает приоритет государственных интересов как общих интересов всех субъектов. Ориентация на свободы, права и интересы граждан не принижает роль государства в обеспечении национальной безопасности в целом и в области информационной безопасности в частности);
3. Неотвратимость наказания (выполняет роль важнейшего профилактического инструмента в решении вопросов правового обеспечения).

Зарубежное законодательство в области информационной безопасности

- Закон **РФ** "Об информации, информатизации и защите информации".
- **США** "Закон об информационной безопасности" (Computer Security Act of 1987).
- **ФРГ** "Закон о защите данных" (Federal Data Protection Act of 1990).
- **Великобритания** – семейство добровольных стандартов BS 7799

Общегосударственные документы РБ

- Конституция РБ
- Закон РБ от 6 сентября 1995 г. № 3850-XII “Об информатизации”;
- Закон РБ от 29 ноября 1994 г. № 3411-XII “О государственных секретах”;
- Закон РБ от 3 декабря 1997 г. № 102-З “Об органах государственной безопасности Республики Беларусь”;
- Постановление Совета Министров РБ от 15 февраля 1999 г. № 237 “О служебной информации ограниченного распространения”;
- Постановление Совета Министров РБ от 10 февраля 2000 г. № 186 “О некоторых мерах по защите информации в Республике Беларусь”;
- Указ Президента Республики Беларусь от 12 мая 2004 г. № 231 “Вопросы Государственного центра безопасности информации

- Гражданин имеет право на ознакомление с документами, затрагивающими его права и свободы, получение информации обо всех сторонах жизнедеятельности государства, если иное не предусмотрено законом.
- Статьи Конституции гарантируют право на личную и семейную тайну, на тайну переписки и иных сообщений, право свободно искать, получать, передавать, производить и распространять информацию любым законным способом.
- Информация составляет **служебную** или **коммерческую** тайну – имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности.

Закон «Об информатизации»

Закон "Об информатизации»:

- ✔ определяет основные понятия в области информатизации;
- ✔ регулирует правоотношения, возникающие в информационной сфере;
- ✔ определяет порядок защиты информационного ресурса, а также прав и обязанностей субъектов, принимающих участие в процессах информатизации.

Действие настоящего Закона не распространяется на отношения, возникающие при создании и функционировании печати и иных средств массовой информации, и на отношения по обработке недокументированной информации.

Закон "О государственных секретах"

Гражданам Республики Беларусь гарантируется право на получение, хранение и распространение полной, достоверной и своевременной информации по всем вопросам жизнедеятельности государства и общества. Наряду с этим требуется ограничение распространения определенных сведений, относящихся к обеспечению национальных интересов государства и общества, их безопасности и обороноспособности, преждевременное предание гласности которых может нанести ущерб Республике Беларусь.

Конституционное право граждан на получение, хранение и распространение информации может быть ограничено только законом.

Настоящий Закон определяет правовые основы отнесения сведений к государственным секретам и устанавливает единую систему защиты государственных секретов во всех видах деятельности органов законодательной, исполнительной и судебной власти, органов местного управления и самоуправления, органов государственного контроля и надзора, юридических лиц независимо от форм собственности, а также физических лиц на всей территории Республики Беларусь и в ее учреждениях за рубежом.

Основные понятия закона

- **Государственные секреты** — защищаемые государством сведения, распространение которых может нанести ущерб национальной безопасности, обороноспособности и жизненно важным интересам Республики Беларусь. Государственные секреты являются собственностью Республики Беларусь.
- **Защита государственных секретов** — принятие предусмотренных настоящим Законом и подзаконными актами правовых, организационных, инженерно-технических и иных мер по ограничению распространения сведений, отнесенных в установленном порядке к государственным секретам. Защита государственных секретов — обязанность всех органов законодательной, исполнительной и судебной власти, государственных органов, юридических, а также физических лиц, имеющих их.

- **Разглашение государственных секретов** — передача, предоставление, пересылка, утрата носителей секретной информации, а также сообщение, публикация и доведение государственных секретов любыми другими способами до юридических и физических лиц, которым не предоставлено **право ознакомления с ними**.
- **Утрата государственных секретов** — выход сведений, составляющих государственные секреты, из законного владения или пользования в результате утери либо хищения.
- **Носители сведений, составляющих государственные секреты**, — имеющие их физические лица, а также материальные объекты (документы, изделия и т. п.), в том числе физические поля, в которых содержатся сведения, составляющие государственные секреты.

Категории государственных секретов

- **Государственная тайна** — государственные секреты, разглашение или утрата которых может повлечь тяжкие последствия для национальной безопасности, обороноспособности, экономических и политических интересов Республики Беларусь, а также создать реальную угрозу безопасности правам и свободам граждан.
- **Служебная тайна** — государственные секреты, разглашение или утрата которых может нанести ущерб национальной безопасности, обороноспособности, политическим и экономическим интересам Республики Беларусь, а также правам и свободам граждан.

Сведения, составляющие служебную тайну, как правило, имеют характер отдельных данных, входящих в состав сведений, являющихся государственной тайной, и не раскрывают ее в целом.

Формы допуска к государственным секретам

- Форма № 1 – форма допуска к сведениям особой важности (гос. тайна) и их носителям;
- Форма № 2 – форма допуска к совершенно секретным сведениям (гос.тайна) и их носителям;
- Форма № 3 – форма допуска к секретным сведениям (служебная тайна) и их носителям.
- Доступ к государственным секретам без оформления допуска на время полномочий предоставляется:
  - Президенту Республики Беларусь;
  - Премьер-министру Республики Беларусь;
  - Депутатам Палаты представителей Национального собрания Республики Беларусь, депутатам местных Советов депутатов, членам Совета Республики Национального собрания РБ;
  - Судьям.

Закон "Об органах государственной безопасности РБ"

Функции органов ГБ:

- ✔ Организация правительственной и оперативной связи
- ✔ Организация и обеспечение безопасности шифрованной, засекреченной и кодированной связи в РБ и ее учреждениях за рубежом
- ✔ Государственный контроль за этой деятельностью
- ✔ Контроль за использованием на территории РБ радиоизлучающих средств и запрещение использования этих средств, работающих с нарушением установленных правил обращения с государственными секретами либо создающих радиопомехи функционированию средств правительственной и оперативной радиосвязи.

Правительственная (телефонная и документальная) и оперативная (телефонная) связь являются специальными системами электрической связи, обеспечивающими секретность передаваемой по ним информации

Правительственная связь организуется в интересах государственных органов.

Оперативная связь организуется в интересах правоохранительных органов.

Постановление Совета Министров "О служебной информации ограниченного распространения"

Законодательно организациям позволено присваивать гриф "Для служебного пользования" сведениям, распространение которых организации считают нежелательными в интересах своей деятельности.

Перечень сведений ограниченного распространения:

- ✔ мобилизационные вопросы;
- ✔ наука и техника;
- ✔ оборона и государственная безопасность;
- ✔ правоохранительная деятельность.

Постановление Совета Министров "О некоторых мерах по защите информации в Республике Беларусь"

Установить, что при обработке информации, отнесенной к госсекретам и служебной информации ограниченного распространения с использованием средств электронно-вычислительной техники, должны применяться защищенные по требованиям безопасности информации компьютерные системы, изготавливаемые, как правило, на предприятиях РБ. В обоснованных случаях могут применяться компьютерные системы импортного производства, прошедшие специальные исследования и обеспеченные защитой, необходимый уровень которой подтвержден сертификатом соответствия.

Указ Президента РБ “Вопросы ГЦБИ при Президенте Республики Беларусь”

Государственный центр безопасности информации при Президенте Республики Беларусь (ГЦБИ) является специально уполномоченным государственным органом, осуществляющим регулирование деятельности по обеспечению защиты информации, содержащей сведения, составляющие государственные секреты Республики Беларусь или иные сведения, охраняемые в соответствии с законодательством, от утечки по техническим каналам, несанкционированных и непреднамеренных воздействий.

ГЦБИ в своей деятельности руководствуется Конституцией и законами Республики Беларусь, декретами и указами Президента Республики Беларусь, постановлениями Совета Безопасности Республики Беларусь, настоящим Положением, другими актами законодательства Республики Беларусь, а также международными договорами Республики Беларусь.

Общее руководство ГЦБИ осуществляется Президентом Республики Беларусь.

Основные задачи ГЦБИ:

1. Информирование Президента Республики Беларусь о внешних и внутренних угрозах информационной безопасности страны;
2. Обеспечение технической защиты информации в местах постоянного и временного пребывания Президента Республики Беларусь, а также постоянных членов Совета Безопасности Республики Беларусь;
3. Предотвращение утечки по техническим каналам информации, содержащей государственные секреты или иные сведения, охраняемые в соответствии с законодательством Республики Беларусь, несанкционированных и непреднамеренных воздействий на нее;
4. Организация и осуществление контроля деятельности по обеспечению технической защиты информации в государственных органах, организациях независимо от организационно-правовых форм и форм собственности;
5. Организация и проведение сертификации, аттестации, экспертизы и лицензирования в области технической защиты информации.

Концепция национальной безопасности Республики Беларусь

Концепция национальной безопасности Республики Беларусь (утверждена Указом Президента Республики Беларусь 17.07.2001 № 390) состоит из 8 частей и представляет собой систему взглядов относительно направлений, средств и способов защиты жизненно важных интересов личности, общества и государства. Концепция содержит методологическую основу построения системы обеспечения национальной безопасности Республики Беларусь и предназначена для использования при планировании и осуществлении деятельности государственных органов по обеспечению национальной безопасности.

Шестая часть данного документа посвящена безопасности Республики Беларусь в информационной сфере и содержит сформулированные жизненно важные интересы и основные факторы, создающие угрозу безопасности в данной сфере, определены приоритетные направления обеспечения безопасности в Республике Беларусь.

Жизненно важные интересы Республики Беларусь в информационной сфере:

1. Обеспечение информационных потребностей личности, общества и государства во всех сферах их жизнедеятельности;
2. Обеспечение прав граждан на тайну корреспонденции, телефонных и иных сообщений;
3. Эффективное использование, поддержание сохранности и систематическое пополнение национальных информационных ресурсов;
4. Защита сведений, составляющих государственную, служебную, коммерческую и иную охраняемую законодательством тайну;
5. Развитие информационных технологий, средств информатизации и связи;
6. Обеспечение безопасности информационных систем и сетей связи;
7. Участие государства в работе международных организаций в информационной области.

Основные факторы, создающие угрозу безопасности Республики Беларусь в информационной сфере

1. Распространение недостоверной информации, направленное на дестабилизацию в Республике Беларусь;
2. Зависимость информационной инфраструктуры государства от импорта зарубежных информационных технологий, систем информатизации и связи, программного обеспечения;
3. Недостаточная обеспеченность квалифицированными кадрами в области информационных технологий и защиты информации;
4. Несоответствие информационного обеспечения государственных и общественных институтов современным требованиям управления различными процессами;
5. Недостаточное развитие системы государственного лицензирования, сертификации и аттестации в соответствии с требованиями информационной безопасности;
6. Рост числа преступлений в информационной сфере;
7. Отсутствие эффективной системы обеспечения сохранности открытой информации, в том числе представляющей интеллектуальную собственность.

Приоритетные направления обеспечения безопасности Республики Беларусь в информационной сфере:

1. Совершенствование механизмов реализации прав граждан на получение информации, форм и способов взаимодействия государства со средствами массовой информации. Обеспечение доступа к открытым информационным ресурсам;
2. Разработка и внедрение современных методов и средств защиты информационных технологий;
3. Осуществление государственного контроля за разработкой, созданием, развитием и использованием средств защиты информации;
4. Обеспечение правовых и организационных условий пресечения преступлений в информационной сфере;
5. Участие государства в международных соглашениях регулирующих информационный обмен с использование глобальных информационных сетей и систем.

Правовая защита от компьютерных преступлений

В 1983 г. Международная организация экономического сотрудничества и развития определила под термином “**компьютерная преступность**” (или "связанная с компьютерами преступность") любые незаконные, неэтичные или неправомерные действия, связанные с автоматической обработкой данных и/или их передачей.

С целью унификации национальных законодательств в 1989 г. Комитетом министров Европейского Совета был согласован и утвержден Список правонарушений, рекомендованный странам - участницам ЕС для разработки единой уголовной стратегии по разработке законодательства, связанного с компьютерными преступлениями. Рекомендованный Европейским Советом Список компьютерных преступлений включает в себя так называемые “Минимальный” и “Необязательный списки нарушений”.

"Минимальный список нарушений"

- Компьютерное мошенничество.
- Подделка компьютерной информации.
- Повреждение данных ЭВМ или программ ЭВМ.
- Компьютерный саботаж.
- Несанкционированный доступ.
- Несанкционированный перехват данных.
- Несанкционированное использование защищенных компьютерных программ.
- Несанкционированное воспроизведение схем.

"Необязательный список нарушений"

- Незаконное изменение данных ЭВМ или программ ЭВМ;
- Компьютерный шпионаж;
- Неразрешенное использование ЭВМ.

В Уголовный кодекс РБ включен раздел XII "Преступления против информационной безопасности" .

Организационные методы ЗИ

Государственное регулирование в области защиты информации:

- ограничение доступа к информации есть исключение из общего принципа открытости информации, и осуществляется только на основе законодательства;
- доступ к какой-либо информации осуществляется с учетом определяемых законом прав собственности на эту информацию;
- юридические и физические лица, собирающие, накапливающие и обрабатывающие персональные данные, и конфиденциальную информацию, несут ответственность перед законом за их сохранность и использование;
- государство формирует национальную программу информационной безопасности и создает единую систему информационной безопасности страны;

- государство формирует нормативно-правовую базу в информационной сфере;
- государство осуществляет контроль за созданием и использованием средств защиты информации посредством их обязательной сертификации и лицензирования деятельности в области защиты информации;
- государство поддерживает интернационализацию глобальных информационных сетей и систем;
- государство поддерживает деятельность отечественных производителей средств информатизации и защиты информации.

Система информационной безопасности

является составной частью общей системы национальной безопасности страны и представляет собой совокупность органов государственной власти и управления и предприятий, согласованно осуществляющих деятельность по обеспечению информационной безопасности. В систему входят:

- **органы государственной власти и управления**, решающие задачи обеспечения информационной безопасности в пределах своей компетенции;
- **государственные и межведомственные комиссии и советы**, специализирующиеся на проблемах информационной безопасности;
- **структурные и межотраслевые подразделения** по защите информации **органов государственной власти и управления**, а также структурные подразделения предприятий, проводящие работы с использованием сведений, отнесенных к государственной тайне, или специализирующиеся в области защиты информации;
- **научно-исследовательские, проектные и конструкторские организации**, выполняющие работы по обеспечению информационной безопасности;
- **учебные заведения**, осуществляющие подготовку кадров для работы в системе обеспечения информационной безопасности.

Государственная система защиты информации РБ

- Государственный центр безопасности информации (ГЦБИ);
- структурные подразделения по защите информации органов государственного управления, предприятий, организаций и учреждений;
- головные предприятия (организации, учреждения) по направлениям защиты информации;
- сертификационные и испытательные центры (лаборатории), предприятия, учреждения и организации различных форм собственности по оказанию услуг в области защиты информации.

Основные функции системы информационной безопасности

- разработка и реализация стратегии обеспечения информационной безопасности;
- оценка состояния информационной безопасности в стране, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения и нейтрализации этих угроз;
- координация и контроль деятельности субъектов системы информационной безопасности.

Основные организационные мероприятия по ЗИ в общегосударственных компьютерных системах и сетях

- ***лицензирование*** деятельности предприятий в области защиты информации;
- ***аттестация*** объектов информатизации по выполнению требований обеспечения защиты информации;
- ***сертификация*** средств защиты информации и контроль за ее эффективностью в части защищенности информации от утечки по техническим каналам;
- введение территориальных, частотных, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;
- создание и применение защищенных информационных и автоматизированных систем управления.

Основные виды лицензируемой деятельности

- разработка, производство, монтаж, наладка технических и программно-аппаратных средств защиты информации
- специальные исследования технических средств
- работы по контролю защищенности информации

Основные требования к организациям, претендующим на получение лицензии в области ЗИ:

- уровень квалификации специалистов;
- наличие и качество измерительной базы;
- наличие и качество производственных помещений;
- наличие режимного органа и обеспечению охраны материальных ценностей и секретов заказчика (при необходимости);
- наличие нормативно-технической и методической документации в лицензируемой области деятельности.

Сертификация и аттестация средств ЗИ

Технические и программные средства защиты информационных ресурсов подлежат **обязательной** сертификации.

Органом по сертификации средств защиты информации в республике является ГЦБИ.

Документами, регламентирующими вопросы сертификации в РБ, являются:

- **ГОСТ РБ "Национальная система сертификации РБ";**
- **СТБ 5.1.01-96 "Основные положения";**
- **СТБ 5.1.02-96 "Общие требования и порядок аккредитации";**
- **СТБ 5.1.03-96 "Органы по сертификации систем качества. Общие требования и порядок аккредитации";**
- **СТБ 5.1.04-96 "Порядок проведения сертификации продукции. Общие требования";**
- **СТБ 5.1.05-96 "Сертификация систем качества. Порядок проведения";**
- **СТБ 5.1.06-96 "Положение об экспертах-аудиторах по качеству";**
- **СТБ 5.1.07-96 "Реестр. Общие требования и порядок ведения".**

Функции органа по сертификации:

- ✔ разработка нормативных документов на средства защиты и классификация их по функциональным свойствам;
- ✔ разработка нормативных документов на методы испытаний средств защиты и их гармонизация с аналогичными зарубежными документами;
- ✔ выбор способов подтверждения соответствия средств защиты информации требованиям нормативных документов;
- ✔ сертификация средств защиты информации и выдача сертификатов на их применение;
- ✔ ведение реестра сертифицированных средств защиты информации;
- ✔ инспекционный контроль за качеством продукции, которой присвоен тот или иной класс (уровень) защитных свойств;
- ✔ приостановка или отмена действия выданных сертификатов.

Организационно-административные методы ЗИ

- регламентируют процессы создания и эксплуатации информационных объектов, а также взаимодействие пользователей и систем таким образом, чтобы несанкционированный доступ к информации становился либо невозможным, либо существенно затруднялся

- Организация документооборота конфиденциальной информации (порядок хранения, ознакомления, копирования);
- Выделение специальных помещений и ЭВМ для хранения, обработки и т.д. конфиденциальной информации;
- Использование специальных защищенных программ
- …

Организационно-технические методы ЗИ

- ограничение доступа посторонних лиц внутрь за счет установки механических запорных устройств или замков;
- отключение персональных компьютеров от локальной сети или сети удаленного доступа (региональные и глобальные вычислительные сети) при обработке конфиденциальной информации;
- использование жидкокристаллических мониторов, струйных принтеров или термопечати с целью снижения утечки информации по электромагнитному каналу;
- размещение оборудования для обработки конфиденциальной информации на расстоянии не менее 2,5 м от устройств освещения, связи, металлических труб, теле- и радиоаппаратуры;
- организация электропитания персональных компьютеров от отдельного блока питания (с защитой от побочных электромагнитных излучений или через фильтр напряжения), использование бесперебойных источников питания (БИП).

Страхование как метод ЗИ

- Заключение (сертификат) банковского сертификационного центра является основой для системы страховых гарантий.

- электронного документооборота при заключении и исполнении договоров с участием банков, при оформлении первичных платежных документов с применением цифровой (электронной) подписи;
- от несанкционированного доступа в информационную сеть;
- от разрушения или потери информации в результате программных или аппаратных сбоев;
- от прямых убытков, связанных с незаконным использованием программных и аппаратных средств информационной системы;
- от потерь рабочего времени и ухудшения качества обслуживания клиентов, вызванных поломками или некорректным функционированием аппаратных средств.