

Тема 1

Основные понятия
и принципы защиты информации

Преподаватель



Буй Павел Михайлович

доцент, к.т.н., доцент кафедры
«Автоматика, телемеханика и связь»

Структура курса

- Тема 1. Основные понятия и принципы защиты информации;
- Тема 2. Угрозы, уязвимости и риски информационной безопасности телекоммуникационных систем;
- Тема 3. Методы защиты информации в телекоммуникационных системах;
- Тема 4. Криптографические методы защиты информации в телекоммуникационных системах;
- Тема 5. Средства аутентификации субъектов и управление доступом;
- Тема 6. Сетевая безопасность;
- Тема 7. Защита информации критически важных объектов информатизации;
- Тема 8. Комплексный подход при организации защиты информации.

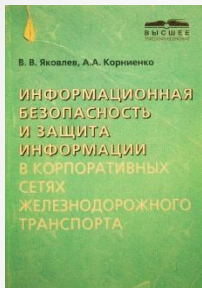
Объем дисциплины

- **Лекции** – один раз в неделю;
- **Практические работы** – один раз в неделю;

Отчетность:

- защита отчета по практическим работам;
- зачет.

Литература



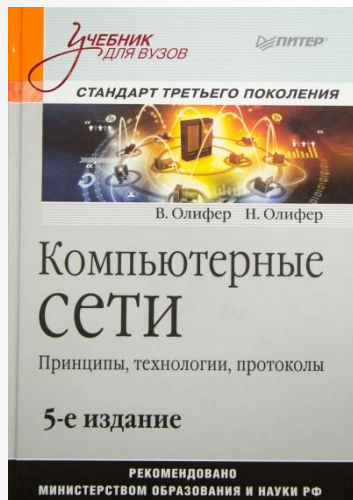
Яковлев, В. В. Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта / В. В. Яковлев, А. А. Корниенко // Учебник для ВУЗов ж.-д. транспорта. – М.: УМК МПС России, 2002. – 328 с.

Романец, Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. – М.: Радио и связь, 2001. – 376с.

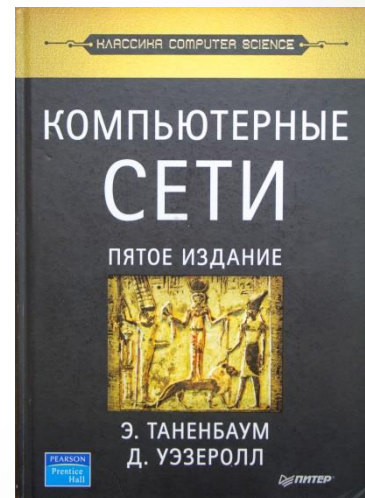


Смит, Ричард Э. Аутентификация: от паролей до открытых ключей / Ричард Э. Смит. – М.: Издательский дом «Вильямс», 2002. – 432с.

Литература

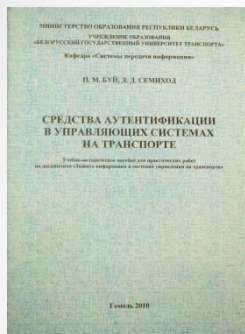


Олифер, В. Компьютерные сети. Принципы, технологии, протоколы / В. Олифер, Н. Олифер // Учебник для ВУЗов. 5-е изд. – СПб. : Питер, 2016. – 992 с.



Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Д. Узеролл // 5-е изд. – СПб. : Питер, 2012. – 960 с.

Литература



Буй, П.М. Средства аутентификации в управляющих системах на транспорте : учеб.-метод. пособие для практ. работ по дисциплине «Защита информации в системах управления на транспорте» / П.М. Буй, Д.Д. Семиход. – Гомель : БелГУТ, 2010. – 39 с.

Буй, П.М. Криптографические методы защиты информации в управляющих системах на транспорте : учеб.-метод. пособие для практ. работ по дисциплине «Защита информации в телекоммуникационных системах» / П.М. Буй, В.О. Матусевич. – Гомель : БелГУТ, 2011. – 56 с.



Белоусова, Е.С. Политика безопасности информационных систем : учеб.-метод. пособие для практ. работ / Е.С. Белоусова, П.М. Буй. – Гомель : БелГУТ, 2016. – 38 с.

Содержание темы

- Основные понятия информационной безопасности (Государственный стандарт Республики Беларусь 50922-2000 «Защита информации. Основные термины и определения»);
- Особенности информации, как объекта защиты;
- Виды информации в соответствии с Законом Республики Беларусь «Об информации, информатизации и защите информации»;

Содержание темы

- Краткий исторический экскурс по вопросам информационной безопасности;
- Задачи в сфере обеспечения информационной безопасности.

Основные понятия информационной безопасности

Существует множество понятий в сфере информационной безопасности, наиболее значимые из которых сформулированы в государственных стандартах и законах, посвященных тематике защиты информации.

К ним, например, относятся:

- государственный стандарт Республики Беларусь 50922-2000 «Защита информации. Основные термины и определения»;
- закон Республики Беларусь № 455-З «Об информации, информатизации и защите информации»;
- Концепция Национальной безопасности Республики Беларусь.

Основные понятия информационной безопасности

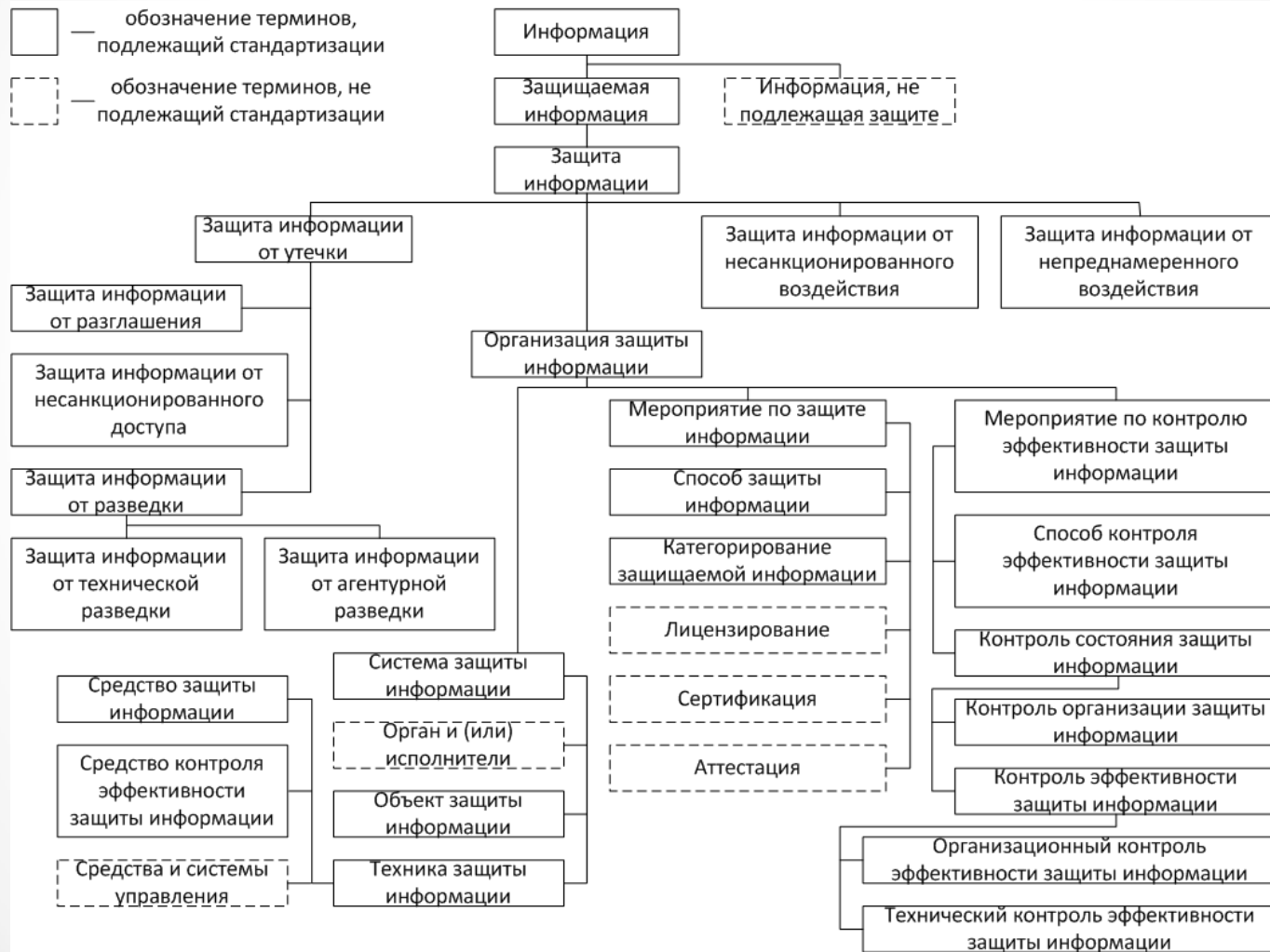
Информационная безопасность - состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

Понятие дано в соответствии с Концепцией Национальной безопасности Республики Беларусь.

Информационная безопасность – это широкое понятие, которым, например, может раскрываться так:

Информационная безопасность - это процесс обеспечения конфиденциальности, доступности, целостности и информации.

СТБ ГОСТ Р 50922-2000



СТБ ГОСТ Р 50922-2000

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником (государство, юридическое лицо, группа физических лиц или отдельное физическое лицо) информации.

Важно:

Защищаемая информация - это

- 1) информация, являющаяся предметом собственности;
- 2) информация, подлежащая защите в соответствии с требованиями...

СТБ ГОСТ Р 50922-2000

Защита информации (ЗИ) – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Нарушение защиты информации происходит в результате:

- 1) утечки защищаемой информации;
- 2) несанкционированных воздействий на защищаемую информацию;
- 3) непреднамеренных воздействий на защищаемую информацию.

СТБ ГОСТ Р 50922-2000

Защита информации от утечки – деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее **разглашения, несанкционированного доступа (НСД)** к информации и получения защищаемой информации **разведками**.

Защита информации от несанкционированного доступа (НСД) – деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом (государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо) с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

СТБ ГОСТ Р 50922-2000

Эффективность защиты информации – степень соответствия результатов защиты информации поставленной цели.

Показатель эффективности защиты информации – мера или характеристика для оценки эффективности защиты информации.

СТБ ГОСТ Р 50922-2000

Система защиты информации – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации.

Средство защиты информации – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Особенности информации, как объекта защиты

Комплекс проблем, связанных с информационной безопасностью, включает в себя не только технические, программные и технологические аспекты защиты информации, но и вопросы защиты прав на нее.

Таким образом, информация может рассматриваться как **объект права собственности**.

Особенности информационной собственности:

- информация не является материальным объектом;
- информация копируется с помощью материального носителя, т. е. является перемещаемой;
- информация является отчуждаемой от собственника.

Особенности информации, как объекта защиты

Право собственности на информацию включает правомочия собственника, к которым относятся:

- право распоряжения;
- право владения;
- право пользования.

Правовое обеспечение защиты информации включает:

- правовые нормы, методы и средства защиты охраняемой информации в Республике Беларусь;
- правовые основы выявления и предупреждения утечки охраняемой информации;
- правовое регулирование организации и проведения административного расследования по фактам нарушения порядка защиты информации.

Особенности информации, как объекта защиты

Документы, регламентирующие информацию в качестве объекта права:

- Гражданский кодекс Республики Беларусь;
- Закон Республики Беларусь № 455-З «Об информации, информатизации и защите информации»;
- Закон Республики Беларусь № 170-З «О государственных секретах».

Виды информации

Закон Республики Беларусь № 455-З «Об информации, информатизации и защите информации» от 10 ноября 2008 г.

Статья 2. Настоящим Законом регулируются общественные отношения, возникающие при:

- поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, а также пользовании информацией;
- создании и использовании информационных технологий, информационных систем и информационных сетей, формировании информационных ресурсов;
- организации и обеспечении защиты информации.

Виды информации

Глава 3. Правовой режим информации

Статья 15. Виды информации.

В зависимости от категории доступа информация делится на:

- общедоступную информацию;
- информацию, распространение и (или) предоставление которой ограничено.

Виды информации

Статья 16. Общедоступная информация

К общедоступной информации относится информация, доступ к которой, распространение и (или) предоставление которой не ограничены.

Примеры:

- информация о правах, свободах и законных интересах физических лиц, правах и законных интересах юридических лиц и о порядке реализации прав, свобод и законных интересов;
- о состоянии здравоохранения, демографии, образования, культуры, сельского хозяйства;
- о размерах золотого запаса;

и т. п.

Виды информации

Статья 17. Информация, распространение и (или) предоставление которой ограничено.

К информации, распространение и (или) предоставление которой ограничено, относится:

- информация о частной жизни физического лица и персональные данные;
- сведения, составляющие государственные секреты;
- информация, составляющая **коммерческую** и **профессиональную** тайну;
- информация, содержащаяся в делах об административных правонарушениях, материалах и уголовных делах органов уголовного преследования и суда до завершения производства по делу;
- иная информация, доступ к которой ограничен законодательными актами Республики Беларусь.

Виды информации

Статья 18. Информация о частной жизни физического лица и персональные данные.

Никто не вправе требовать от физического лица предоставления информации о его **частной жизни** и персональных данных, включая сведения, составляющие **личную и семейную тайну, тайну телефонных переговоров, почтовых и иных сообщений, касающиеся состояния его здоровья**, либо получать такую информацию иным образом помимо воли данного физического лица, кроме случаев, установленных законодательными актами Республики Беларусь.

Сбор, обработка, хранение информации о частной жизни физического лица и персональных данных, а также пользование ими осуществляются с **согласия** данного физического лица, если иное не установлено законодательными актами Республики Беларусь.

Краткий исторический Экскурс

Исторически сложилось так, что вопросы информационной безопасности базировались на вопросах криптографии. Поэтому исторический экскурс удобно увязать с историей криптографии.

История криптографии насчитывает около 4 тысяч лет. В качестве основного критерия периодизации криптографии используются технологические характеристики методов шифрования.

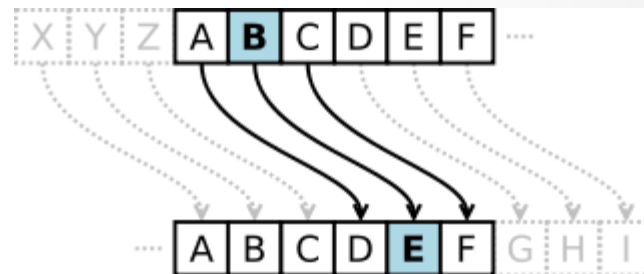
Краткий исторический Экскурс

Первый период (приблизительно с 3-го тысячелетия до н. э.).

Характеризуется господством **моноалфавитных** шифров, основной принцип которых – это замена алфавита исходного текста другим алфавитом через замену букв другими буквами или символами.

Примеры:

- скитала;
- шифр Цезаря;
- искусство млечхита-викальпа и т. п.



Краткий исторический Экскурс

Второй период (с IX века на Ближнем Востоке и с XV века в Европе - до начала XX века).

Характеризуется введением в обиход **полиалфавитных** шифров.

Примеры:

- диск Альберти;
- шифр Виженера;
- дисковый шифр Джефферсона и т. п.



| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | а | б | в | г | д | е | ж | з |
| а | ъ | щ | г | й | н | ю | ж | а |
| б | щ | ш | в | и | м | э | е | я |
| в | ш | ч | б | з | л | ь | д | ю |
| г | ч | ц | а | ж | к | ы | г | э |
| д | ц | х | я | е | й | ъ | в | ь |
| е | х | ф | ю | д | и | щ | б | ы |
| ж | ф | у | э | г | з | ш | а | ъ |
| з | у | т | ь | в | ж | ч | я | щ |



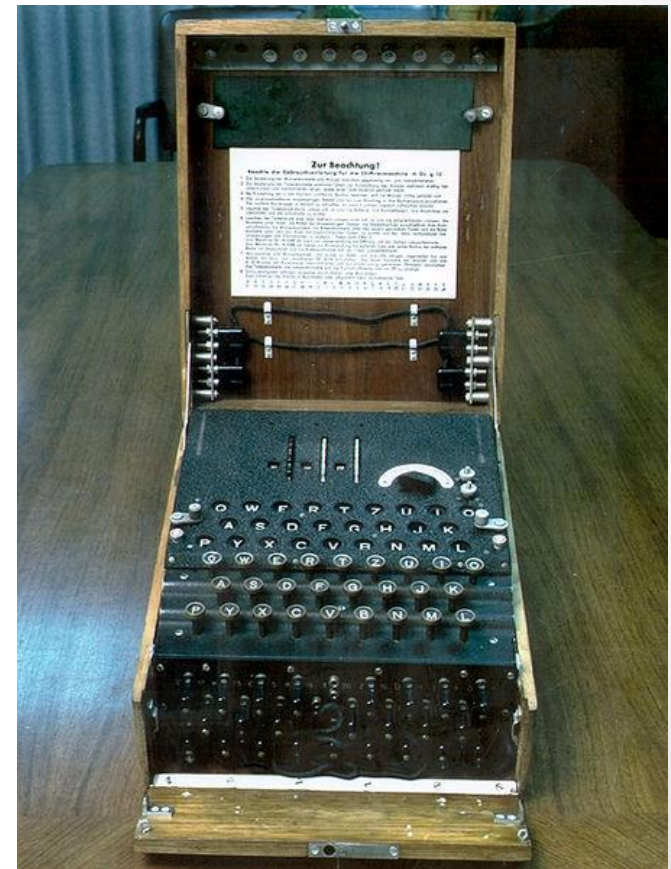
Краткий исторический Экскурс

Третий период (с начала и до середины XX века).

Характеризуется внедрением электромеханических устройств в работу шифровальщиков. При этом продолжалось использование **полиалфавитных** шифров.

Шифровальные машины:

- «Энигма» Германия;
- «Purple» Япония;
- M-209 США;
- K-37 «Кристалл» СССР и т. п.



Краткий исторический Экскурс

Четвёртый период (с середины до 70-х годов XX века).

Характеризуется переходом к математической криптографии. Обязательным этапом создания шифра считается изучение его уязвимости к различным известным атакам. Однако до 1975 года криптография оставалась «классической» или же, более корректно, **криптографией с секретным ключом**.

Криптографические алгоритмы:

- DES (1976), AES (2001);
- ГОСТ 28147-89 (1989);
- TEA (1994), Twofish (1998), IDEA (2000) и т. п.

Краткий исторический Экскурс

Современный период развития криптографии (с конца 1970-х годов по настоящее время).

Характеризуется зарождением и развитием нового направления - **криптографией с открытым ключом**. Практическое применение криптографии стало неотъемлемой частью жизни современного общества (электронная коммерция, электронный документооборот, телекоммуникации).

Криптографические алгоритмы:

- RSA (1977);
- Эль-Гамаль (1985) и т. п.

Задачи в сфере обеспечения ИБ

Для эффективного обеспечения безопасности информации требуется создание развитого методологического базиса, позволяющего решить следующие комплексные задачи:

1. Создать систему органов, ответственных за безопасность информации;
2. Разработать теоретико-методологические основы обеспечения безопасности информации;
3. Решить проблему управления защитой информации и ее автоматизации;

Задачи в сфере обеспечения ИБ

4. Создать нормативно-правовую базу, регламентирующую решение всех задач обеспечения безопасности информации;
5. Наладить производство средств защиты информации;
6. Организовать подготовку специалистов по защите информации;
7. Подготовить нормативно-методическую базу для проведения работ по обеспечению безопасности информации.

Задачи в сфере обеспечения ИБ

Комплексные задачи обеспечения безопасности информации

| Задача | Цель решения | Общее содержание |
|--|--|--|
| 1 Создание системы органов, ответственных за безопасность и информации | Создание стройной системы органов, необходимых и достаточных для эффективного решения всех задач обеспечения безопасности информации на общегосударственном, региональном (ведомственном) и объектовом уровнях | Создание органов, осуществляющих: –управление процессами обеспечения безопасности; –проведение научно-исследовательской работы; –разработку и производство необходимых средств; –практическое решение задач обеспечения безопасности информации на объектах; –подготовку, повышение квалификации и переподготовку кадров. |

Задачи в сфере обеспечения ИБ

Комплексные задачи обеспечения безопасности информации

| Задача | Цель решения | Общее содержание |
|---|---|--|
| 2 Разработка теоретико-методологического базиса обеспечения безопасности информации | Создание научно обоснованного базиса решения всех задач, связанных с обеспечением безопасности информации | <p>Обоснование понятийного аппарата. Аналитико-синтетическая обработка имеющихся данных.</p> <p>Обоснование современной постановки задачи.</p> <p>Обоснование стратегических подходов к обеспечению безопасности.</p> <p>Разработка методов решения задач обеспечения безопасности.</p> <p>Обоснование структуры и содержания инструментально-методологической базы решения задач.</p> <p>Обоснование путей и способов решения задач обеспечения безопасности.</p> <p>Обоснование перспектив развития теории и практики обеспечения безопасности информации.</p> |

Задачи в сфере обеспечения ИБ

Комплексные задачи обеспечения безопасности информации

| Задача | Цель решения | Общее содержание |
|---|---|---|
| 3 Решение проблемы управления защитой информации и ее автоматизации | Разработка методов и технологии управления защитой информации | <p>Отработка принципов управления в рамках государственной СЗИ:</p> <ol style="list-style-type: none">1) по трем основным уровням:<ul style="list-style-type: none">– во взаимодействии со структурами государственной власти;– в регионах, территориально-промышленных зонах;– на предприятиях, полигонах, объектах, в системах и комплексах.2) в двух состояниях (режимах):<ul style="list-style-type: none">– повседневном (режим заблаговременного, планового осуществления мер по ЗИ);– «быстрого реагирования» (режим принятия оперативных решений и осуществления мер по ЗИ). <p>Создание систем управления защитой информации различного уровня и назначения.</p> |

Задачи в сфере обеспечения ИБ

Комплексные задачи обеспечения безопасности информации

| Задача | Цель решения | Общее содержание |
|---|---|--|
| 4 Создание нормативно-правовой базы, регламентирующей решение задач обеспечения безопасности информации | Создание условий, необходимых для правового и нормативного регулирования решения всех задач обеспечения безопасности информации | Обоснование структуры и содержания нормативно-правовой базы. Разработка и организация принятия законов, регламентирующих деятельность в области обеспечения безопасности информации. Разработка, утверждение и распространение системы общегосударственных руководящих и методических материалов по обеспечению безопасности информации. Определение порядка разработки, утверждения региональных (ведомственных) документов по обеспечению безопасности информации. Разработка, утверждение и распространение комплекта типовых инструкций по решению задач обеспечения безопасности информации. Разработка и узаконивание правил сертификации средств и лицензирования деятельности по обеспечению безопасности информации. |

Задачи в сфере обеспечения ИБ

Комплексные задачи обеспечения безопасности информации

| Задача | Цель решения | Общее содержание |
|---|---|---|
| 5 Организация производства средств защиты информации на промышленной основе | Создание индустрии производства и распространения средств обеспечения безопасности информации | <p>Обоснование перечня и содержания средств обеспечения безопасности.</p> <p>Создание системы предприятий и учреждений, производящих средства обеспечения безопасности.</p> <p>Определение порядка разработки, аттестации и распространения технических средств.</p> <p>Определение порядка разработки, аттестации и распространения программных средств.</p> <p>Определение порядка разработки, аттестации и распространения организационных средств.</p> <p>Определение порядка разработки, аттестации и распространения криптографических средств.</p> |

Задачи в сфере обеспечения ИБ

Комплексные задачи обеспечения безопасности информации

| Задача | Цель решения | Общее содержание |
|---|--|---|
| 6 Организация системы подготовки кадров по безопасности | Создание регулярной системы подготовки специалистов по безопасности информации, необходимого количества и требуемых профилей | Разработка и научное обоснование концепции подготовки кадров по безопасности информации. Определение перечня учебных заведений, уполномоченных готовить кадры по безопасности информации, и распределение между ними функций. Организация подготовки молодых специалистов. Организация повышения квалификации специалистов по безопасности информации. Организация переподготовки специалистов другого профиля. Организация подготовки научно-педагогических кадров в области безопасности информации. Организация всеобуча по безопасности информации. |

Задачи в сфере обеспечения ИБ

Комплексные задачи обеспечения безопасности информации

| Задача | Цель решения | Общее содержание |
|---|---|---|
| 7 Создание системы документационно-методического обеспечения работ по безопасности информации | Создание регулярной системы обеспечения всех органов и специалистов по безопасности информации необходимыми источниками и пособиями | Разработка и научное обоснование системы документационно-методического обеспечения. Создание системы разработки, издания и распространения официальных документов. Создание системы разработки, издания и распространения трудов монографического характера. Создание системы разработки, издания и распространения учебно-методической литературы. Создание системы разработки, издания и распространения периодических изданий. |

Задачи в сфере обеспечения ИБ

Государственная политика в сфере формирования информационных ресурсов и информатизации должна быть направлена на создание условий для эффективного и качественного информационного обеспечения решения стратегических и оперативных задач социального и экономического развития страны.

Задачи в сфере обеспечения ИБ

- Основными направлениями государственной политики в сфере информатизации являются:
 - ✓ обеспечение условий для развития и защиты всех форм собственности на информационные ресурсы;
 - ✓ формирование и защита государственных информационных ресурсов;
 - ✓ создание и развитие и региональных информационных систем и сетей, обеспечение их совместимости и взаимодействия в едином информационном пространстве;

Задачи в сфере обеспечения ИБ

- ✓ создание условий для качественного и эффективного информационного обеспечения граждан, органов государственной власти, организаций и общественных объединений на основе государственных информационных ресурсов;
- ✓ обеспечение национальной безопасности в сфере информатизации, а также обеспечение реализации прав граждан и организаций в условиях информатизации;

Задачи в сфере обеспечения ИБ

- ✓ содействие формированию рынка информационных ресурсов, услуг, информационных систем, технологий и средств их обеспечения;
- ✓ формирование и осуществление единой научно-технической и промышленной политики в сфере информатизации с учетом современного мирового уровня развития информационных технологий;
- ✓ поддержка проектов и программ информатизации;
- ✓ создание и совершенствование системы привлечения инвестиций и механизма стимулирования разработки и реализации проектов информатизации;
- ✓ развитие законодательства в сфере информационных процессов, информатизации и защиты информации.