Тема 1

Основные понятия
и терминология защиты информации

Преподаватель

Буй Павел Михайлович

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

Структура курса

- Тема 1. **Основные понятия и терминология защиты информации;**
- Тема 2. **Угрозы и модель нарушителя информационной безопасности;**
- Тема 3. **Правовое обеспечение и государственное регулирование защиты информации в Республике Беларусь;**
- Тема 4. **Методы и средства анализа безопасности программного обеспечения;**
- Тема 5. **Управление доступом к информации в базах данных;**
- Тема 6. **Криптографические методы защиты программного обеспечения и баз данных;**
- Тема 7. **Средства аутентификации при защите программного обеспечения и баз данных;**
- Тема 8. **Комплексный подход к обеспечению безопасности информационных систем.**

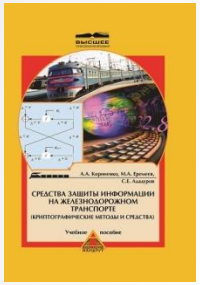
Объем дисциплины

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

Отчетность:

- защита отчета по практическим работам;
- зачет.

Литература

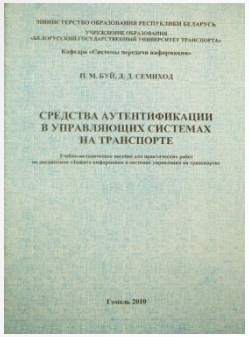


Корниенко, А. А. Средства защиты информации на железнодорожном транспорте (Криптографические методы и средства) : учеб. пособие для вузов / А. А. Корниенко, М. А. Еремеев, С. Е. Ададуров. – М. : Маршрут, 2006. – 252 с.

Щеглов, А. Ю. Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов. – СПб. : Наука и техника, 2005. – 384 с.

Петренко, С. А. Политики информационной безопасности / С. А. Петренко, В. А. Курбатов. – М. : Компания АйТи, 2006. – 400 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 телекоммуникациооных 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

- 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»;
- Краткий исторический экскурс по вопросам 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

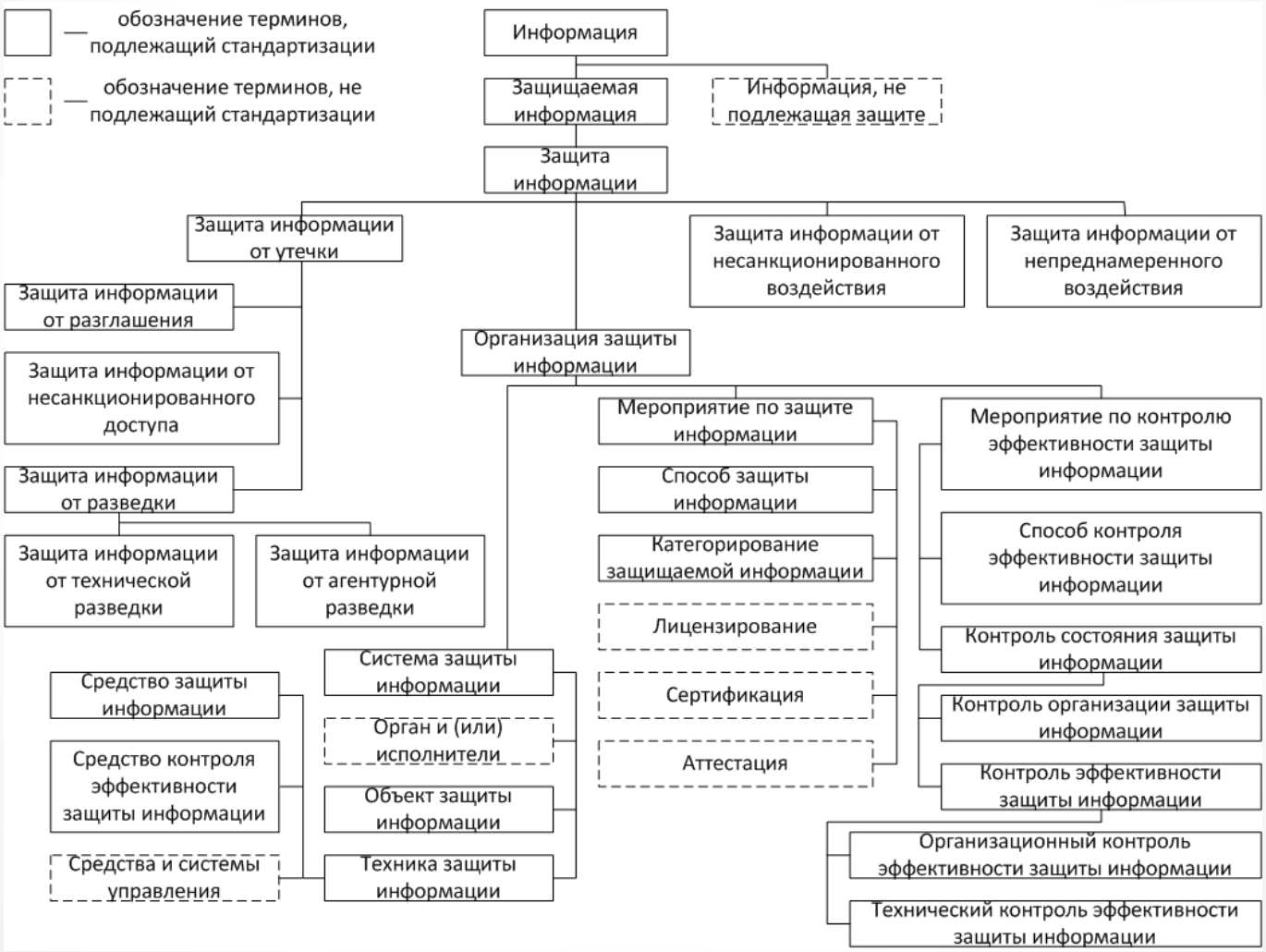
Информационная безопасность - состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

Понятие дано в соответствии с Концепцией Национальной безопасности Республики Беларусь.

Информационная безопасность – это широкое понятие, котором, 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

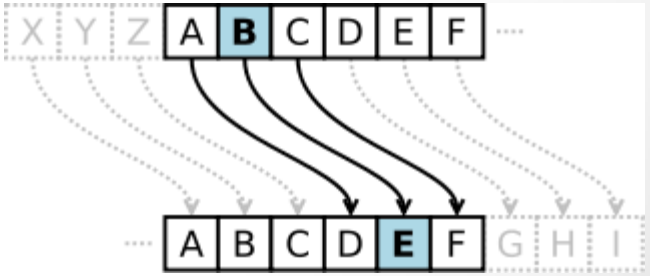
Исторически сложилось так, что вопросы информационной безопасности базировались на вопросах криптографии. Поэтому исторический экскурс удобно увязать с историей криптографии.

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.



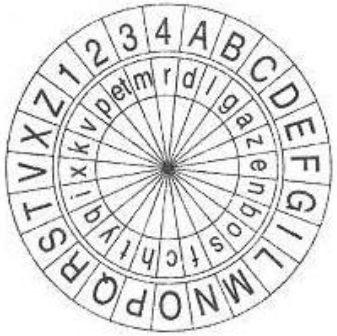
Примеры:

- скитала;
- шифр Цезаря;
- искусство млеччхита-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.



	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

Примеры:

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

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-Гамаля (1985) и т. п.