# Тема 2

Основные понятия и принципы защиты информации

# Содержание темы

- Основные понятия информационной безопасности.
- Государственный стандарт Республики Беларусь 50922-2006 «Защита информации. Основные термины и определения».
- Особенности информации, как объекта защиты.
- *Виды информации в соответствии с Законом Республики Беларусь № 455-З «Об информации, информатизации и защите информации».*

# Содержание темы

- Концепция информационной безопасности Республики Беларусь.
- 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 50922-2006 «Защита информации. Основные термины и определения»;
- закон Республики Беларусь № 455-З «Об информации, информатизации и защите информации»;
- Концепция Информационной 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, которое, например, может раскрываться так:

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

# СТБ ГОСТ Р 50922-2006

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

Важно:

Защищаемая информация - это

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

# СТБ ГОСТ Р 50922-2006

**Защита информации (ЗИ)** – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и преднамеренных 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 50922-2006

**Защита информации от утечки** – защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации [иностранными] разведками и другими заинтересованными субъектами (государство, юридическое лицо, группа физических лиц, отдельное физическое лицо).

# СТБ ГОСТ Р 50922-2006

**Защита информации от несанкционированного доступа (ЗИ от НСД)** – защита информации, направленная на предотвращение получения защи-щаемой информации заинтересованными субъектами (государство, юридическое лицо, группа физических лиц, в том числе общественная орга-низация, отдельное физическое лицо) с нарушением установленных норма-тивными правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

# СТБ ГОСТ Р 50922-2006

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

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

# СТБ ГОСТ Р 50922-2006

**Система защиты информации** – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты ин-формации.

**Средство защиты информации** – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты ин-формации.

# 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.

# Концепция ИБ РБ

Постановление

Совета Безопасности Республики Беларусь

18 марта 2019 г. № 1 г.Минск

О Концепции информационной безопасности Республики Беларусь

Совет Безопасности Республики Беларусь п о с т а н о в л я е т:

1. Утвердить Концепцию информационной безопасности Республики Беларусь (прилагается).

2. Государственным органам и иным организациям в практической деятельности руководствоваться положениями Концепции информационной безопасности Республики Беларусь.

3. Государственному секретарю Совета Безопасности Республики Беларусь отражать результаты реализации Концепции информационной безопасности Республики Беларусь в ежегодном докладе Президенту Республики Беларусь о состоянии национальной безопасности и мерах по ее укреплению.

Президент
Республики Беларусь А.Лукашенко

Для правовых актов

21

# Концепция ИБ РБ

## ГЛАВА 1
## МИРОВОЕ ЗНАЧЕНИЕ ИНФОРМАЦИОННОЙ СФЕРЫ

Индустрия телекоммуникации стала одной из наиболее динамичных и перспективных сфер мировой экономики. С процессами информатизации все больше связываются национальные экономические интересы и перспективы инвестиций.

# Концепция ИБ РБ

## ГЛАВА 10
## ОБУСЛОВЛЕННОСТЬ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

40. Механизмы деструктивного информационно-психологического воздействия на личность, общество и государство постоянно совершенствуются, а масштабное манипулирование массовым сознанием принимает такую же остроту, как борьба за территории, ресурсы и рынки. Через информационное пространство осуществляется преднамеренная дискредитация конституционных основ государств и их властных структур, размывание национального менталитета и самобытности, вовлечение людей в экстремистскую и террористическую деятельность, разжигание межнациональной и межконфессиональной вражды, формирование радикального и протестного потенциала. Информационный фактор играет все более значительную роль в межгосударственных конфликтах и неявных действиях, направленных на нарушение суверенитета, территориальной целостности стран и снижение темпов их развития. В результате информационных воздействий существенно меняются социальные связи человека в обществе, стиль мышления, способы общения, восприятие действительности и самооценка.

# Концепция ИБ РБ

**ГЛАВА 10**
**ОБУСЛОВЛЕННОСТЬ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ**

Все большее беспокойство вызывает активное распространение в информационном пространстве фальсифицированной, недостоверной и запрещенной информации. Снижение критического отношения потребителей информации к фейковым сообщениям новостных ресурсов, в социальных сетях и на других онлайн-платформах создает предпосылки преднамеренного использования дезинформации для дестабилизации общественного сознания в политических, социально-опасных, иных подобных целях.

# Концепция ИБ РБ

**ГЛАВА 15**
**ОБУСЛОВЛЕННОСТЬ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ**

Повсеместное функционирование объектов промышленности, транспорта, энергетики, электросвязи, здравоохранения и систем жизнеобеспечения с автоматизированными системами управления ставит в прямую зависимость жизнь и здоровье населения, экологическую и социальную безопасность от их надежности и защищенности. Кибератаки на информационную инфраструктуру рассматриваются в мире как одна из наиболее значимых угроз безопасности.

Во многих национальных вооруженных силах создаются и развиваются кибервойска, а проведение кибероперации предусматривается в доктринальных и стратегических документах. Одновременно рассматривается возможность реагирования на кибератаки как на вооруженную агрессию, что в условиях практической невозможности точной идентификации их источников (инициаторов) может привести к бездоказательной и произвольной трактовке обоснованности встречных военных действий.

# Концепция ИБ РБ

**ГЛАВА 15**
**ОБУСЛОВЛЕННОСТЬ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ**

Неуклонно растет количество киберпреступлений. Информационные системы и ресурсы становятся как предметом преступлений, так и средством их совершения. Формируется тотальная зависимость финансового сектора и иных секторов от надежности электронных систем хранения, обработки и обмена данными.

60. Однако ни в глобальном, ни в региональных масштабах пока не удается эффективно воспрепятствовать разработкам и распространению средств, заведомо предназначенных для уничтожения, блокирования, модификации, похищения информации в сетях и ресурсах или нейтрализации мер по ее защите. Выработка правовых, процедурных, технических и организационных мер против кибервоздействий на информационные ресурсы отстает от формирования реальных и потенциальных угроз их осуществления.

# Краткий исторический экскурс

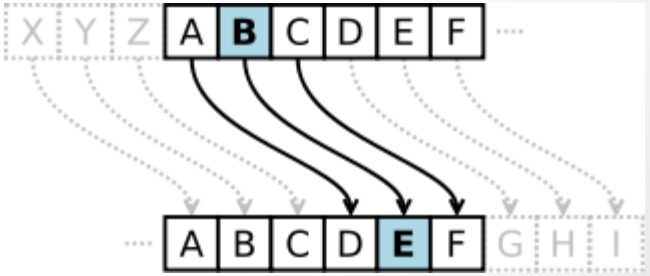
Исторически сложилось так, что вопросы информационной безопасности базировались на вопросах криптографии. Поэтому исторический экскурс удобно увязать с историей криптографии.

**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.



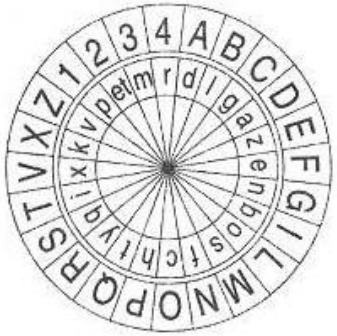

Примеры:

- 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.