УО «ПОЛОЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

К ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

по дисциплине «ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ»

РАЗДЕЛ I
ГОСУДАРСТВЕННЫЕ И МЕЖДУНАРОДНЫЕ СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

НОВОПОЛОЦК 2015

МАТЕРИАЛЫ ПОДГОТОВИЛА:

старший преподаватель кафедры радиоэлектроники

Бураченок Ирина Брониславовна

ПРАКТИЧЕСКАЯ РАБОТА №1

ТЕМА: Технический регламент Республики Беларусь

ЦЕЛЬ РАБОТЫ: Изучить область применения Технического регламента Республики Беларусь, требования к информационной безопасности различных объектов, с сертификацией и др. средств защиты информации.

Результат обучения:

После успешного завершения занятия пользователь должен:

- Знать области применения Технического регламента Республики Беларусь.
- знать требования к информационной безопасности различных объектов.
- изучить особенности сертификации и других средств защиты информации в Республике Беларусь.

Используемая программа: Firefox, Internet Explorer, Opera и др.

План занятия:

1. Изучение кратких теоретических сведений.
2. Выполнение задания.
3. Оформление отчета.

1. КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Технический регламент Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) (утвержден Постановлением Совета Министров Республики Беларусь 15.05.2013 № 375)

Статья 1. Область применения

1. Технический регламент Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) распространяется на выпускаемые в обращение на территории Республики Беларусь средства защиты информации независимо от страны происхождения, за исключением средств шифрованной, других видов специальной связи и криптографических средств защиты государственных секретов.

2. Настоящим техническим регламентом устанавливаются требования к средствам защиты информации в целях защиты жизни и здоровья человека, имущества, а также предупреждения действий, вводящих в заблуждение потребителей (пользователей) относительно назначения, информационной безопасности и качества средств защиты информации.

3. До введения в действие настоящего технического регламента в отношении средств защиты информации, подлежащих согласно законодательству обязательному подтверждению соответствия, применяются правила, установленные Национальной системой подтверждения соответствия Республики Беларусь.

Статья 2. Термины и их определения

В настоящем техническом регламенте применяются следующие термины и их определения:

государственная информационная система – информационная система, создаваемая и (или) приобретаемая за счет средств республиканского или местных

бюджетов, государственных внебюджетных фондов, а также средств государственных юридических лиц;

защита информации – комплекс правовых, организационных и технических мер по обеспечению целостности, конфиденциальности, доступности и сохранности информации;

заявитель на подтверждение соответствия (далее – заявитель) – юридическое лицо Республики Беларусь, иностранное или международное юридическое лицо (организация, не являющаяся юридическим лицом), индивидуальный предприниматель, зарегистрированный в Республике Беларусь, иностранный гражданин или лицо без гражданства, обратившиеся с заявкой на получение сертификата соответствия, либо изготовитель (продавец), обратившийся с заявкой о регистрации принятой им декларации о соответствии;

изготовитель (продавец) – юридическое лицо Республики Беларусь или индивидуальный предприниматель, осуществляющие производство и (или) реализацию средств защиты информации либо представляющие на основании договора интересы иностранного или международного юридического лица (организации, не являющейся юридическим лицом), осуществляющего производство и (или) реализацию средств защиты информации, или интересы иностранного гражданина либо лица без гражданства, постоянно проживающих за пределами Республики Беларусь и осуществляющих производство и (или) реализацию продукции, в части обеспечения соответствия производимой и (или) реализуемой ими продукции требованиям технических нормативных правовых актов в области технического нормирования и стандартизации, либо открытое в установленном порядке на территории Республики Беларусь представительство иностранной организации, осуществляющей производство и (или) реализацию продукции;

импортер – резидент Республики Беларусь, который заключил с нерезидентом Республики Беларусь внешнеторговый договор на передачу средств защиты информации, осуществляет их реализацию и несет ответственность за их соответствие требованиям информационной безопасности;

испытательная лаборатория (центр) – юридическое лицо, аккредитованное для проведения испытаний продукции в определенной области аккредитации;

критические параметры – параметры, связанные с обеспечением безопасности, несанкционированное раскрытие или модификация которых снижает безопасность средства защиты информации или защищаемой им информации;

носитель информации – материальный объект, в котором информация находит свое отображение и (или) хранится;

обращение средств защиты информации на рынке – движение средств защиты информации от изготовителя к потребителю (пользователю), охватывающее все процессы, которые проходят средства защиты информации после завершения их производства;

объект информатизации – средства электронной вычислительной техники вместе с программным обеспечением, в том числе автоматизированные системы различного уровня и назначения, вычислительные сети и центры, автономные стационарные и персональные электронные вычислительные машины, используемые для обработки информации;

применение по назначению – использование средств защиты информации в соответствии с назначением, указанным в эксплуатационных документах;

средства защиты информации – технические, программные, программно-аппаратные средства, предназначенные для защиты информации, а также средства контроля эффективности ее защищенности;

уполномоченный представитель изготовителя – резидент Республики Беларусь, назначенный изготовителем на осуществление действий от его имени при подтверждении соответствия и размещении средств защиты информации на рынке.

Статья 3. Правила размещения на рынке или ввода в эксплуатацию средств защиты информации

Средства защиты информации выпускаются в обращение на рынке в установленном порядке при их соответствии настоящему техническому регламенту, а также другим техническим регламентам, действие которых на них распространяется.

Средства защиты информации, соответствие которых требованиям настоящего технического регламента не подтверждено, не должны быть маркированы знаком соответствия техническому регламенту согласно ТКП 5.1.08-2012 "Национальная система подтверждения соответствия Республики Беларусь. Знаки соответствия. Описание и порядок применения" (далее – ТКП 5.1.08-2012) и не допускаются к выпуску в обращение на рынке.

Статья 4. Требования информационной безопасности

1. Средства защиты информации должны быть разработаны и изготовлены таким образом, чтобы, применяя их по назначению и выполняя требования к эксплуатации и техническому обслуживанию, они обеспечивали:

- выполнение функций в соответствии с эксплуатационными документами;
- защиту от несанкционированного раскрытия и (или) модификации критических параметров;
- контроль целостности конфигурации;
- самотестирование;
- контроль доступа к функциям управления и настройкам;
- сохранение работоспособности при обработке некорректных данных.

2. Наименование и (или) обозначение средств защиты информации (тип, марка, модель), их параметры и характеристики, наименование и (или) товарный знак изготовителя, наименование страны-изготовителя должны быть нанесены непосредственно на средства защиты информации либо их носители, а также указаны в прилагаемых к ним эксплуатационных документах.

3. Если сведения, приведенные в пункте 2 настоящей статьи, невозможно нанести непосредственно на средства защиты информации или их носители, то они могут указываться только в эксплуатационных документах, прилагаемых к средствам защиты информации. При этом наименование изготовителя и (или) его товарный знак, наименование и обозначение средств защиты информации (тип, марка, модель) должны быть нанесены на упаковку.

4. Маркировка средств защиты информации должна быть разборчивой и нанесена на доступную для осмотра поверхность средств защиты информации или их носители.

5. Эксплуатационные документы средств защиты информации должны включать:

- информацию, перечисленную в пункте 2 настоящей статьи;
- информацию о назначении средств защиты информации;
- основные потребительские свойства или характеристики;
- правила и условия безопасной эксплуатации (использования);
- правила и условия хранения, перевозки, реализации, монтажа и утилизации (при необходимости установления требований к ним);
- информацию о мерах, которые следует предпринять при обнаружении неисправности;
- местонахождение изготовителя, информацию для связи с ним;
- наименование и местонахождение уполномоченного представителя изготовителя, импортера, информацию для связи с ним;
- дату изготовления средств защиты информации;
- обязательства изготовителя (уполномоченного представителя изготовителя) по установке, сопровождению и поддержке средств защиты информации.

6. Маркировка и эксплуатационные документы выполняются на государственных языках Республики Беларусь – белорусском и (или) русском.

Статья 5. Обеспечение соответствия требованиям информационной безопасности

1. Соответствие средств защиты информации настоящему техническому регламенту обеспечивается выполнением требований информационной безопасности технического регламента непосредственно либо выполнением требований взаимосвязанных государственных стандартов.

2. Перечень взаимосвязанных с настоящим техническим регламентом государственных стандартов (далее – перечень стандартов) определяет Оперативно-аналитический центр при Президенте Республики Беларусь.

3. Методы исследований (испытаний) средств защиты информации устанавливаются в государственных стандартах, включенных в перечень стандартов, содержащих правила и методы исследований (испытаний), в том числе правила отбора образцов, необходимые для применения и исполнения требований настоящего технического регламента и осуществления оценки (подтверждения) соответствия продукции.

Статья 6. Подтверждение соответствия требованиям информационной безопасности

1. Процедуры подтверждения соответствия средств защиты информации требованиям информационной безопасности выполняются согласно требованиям Национальной системы подтверждения соответствия Республики Беларусь.

2. Перед выпуском в обращение на рынке средства защиты информации должны быть подвергнуты процедуре подтверждения соответствия требованиям информационной безопасности настоящего технического регламента в форме сертификации или декларирования соответствия.

3. Подтверждению соответствия требованиям информационной безопасности настоящего технического регламента путем сертификации подлежат средства защиты информации, которые будут использоваться для:

- технической защиты государственных секретов;
- создания систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено;
- создания систем безопасности критически важных объектов информатизации;
- обеспечения целостности и подлинности электронных документов в государственных информационных системах.

Требования информационной безопасности настоящего технического регламента, на соответствие которым осуществляется сертификация, определяются Оперативно-аналитическим центром при Президенте Республики Беларусь в зависимости от специфики средств защиты информации.

4. Подтверждение соответствия требованиям информационной безопасности настоящего технического регламента средств защиты информации, за исключением указанных в пункте 3 настоящей статьи, осуществляется изготовителем – юридическим лицом Республики Беларусь или уполномоченным представителем изготовителя, зарегистрированным в установленном порядке на территории Республики Беларусь, или импортером путем декларирования соответствия.

5. Сертификацию средств защиты информации, указанных в пункте 3 настоящей статьи, проводит аккредитованный орган по сертификации согласно схемам:

Схема 1с – для серийно выпускаемой продукции;

Схема 2с – для серийно выпускаемой продукции при наличии у изготовителя сертифицированных в Национальной системе подтверждения соответствия Республики Беларусь системы управления качеством и (или) системы управления безопасностью продукции;

Схема 3с – для партии продукции;

Схема 4с – для единичного изделия.

6. Средства защиты информации для подтверждения соответствия представляет заявитель.

7. При проведении аккредитованным органом по сертификации работ по подтверждению соответствия средств защиты информации, указанных в пункте 3 настоящей статьи:

7.1. аккредитованный орган по сертификации:

- проводит анализ документов, представленных заявителем;
- заключает договор на проведение работ по подтверждению соответствия;
- проводит идентификацию средств защиты информации и отбор образцов для испытаний;
- организует проведение испытаний образца (образцов) средств защиты информации в аккредитованной испытательной лаборатории на соответствие требованиям настоящего технического регламента и взаимосвязанных с настоящим техническим регламентом государственных стандартов (при сертификации на соответствие СТБ 34.101.1-2004 "Информационные технологии и безопасность.

Критерии оценки безопасности информационных технологий.

Часть 1. Введение и общая модель (далее – СТБ 34.101.1-2004), СТБ 34.101.2-2004 Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий.

Часть 2. Функциональные требования безопасности (далее – СТБ 34.101.2-2004), СТБ 34.101.3-2004 Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий.

Часть 3. Гарантийные требования безопасности (далее – СТБ 34.101.3-2004) в качестве основы для оценки средств защиты информации используется задание по безопасности);

- проводит анализ состояния производства (схема 1с) или рассмотрение документов, подтверждающих наличие сертифицированных в Национальной системе подтверждения соответствия Республики Беларусь системы управления качеством и (или) системы управления безопасностью продукции (схема 2с);
- выдает сертификат соответствия настоящему техническому регламенту в рамках Национальной системы подтверждения соответствия Республики Беларусь;
- заключает с заявителем соглашение по сертификации (схемы 1с, 2с);
- осуществляет инспекционный контроль за сертифицированной продукцией (схемы 1с, 2с);

7.2. заявитель:

- подает заявку на проведение работ по сертификации продукции с комплектом документов, который включает:
- технические условия (при наличии);
- задание по безопасности и протокол его оценки в испытательной лаборатории (при сертификации на соответствие требованиям СТБ 34.101.1-2004, СТБ 34.101.2-2004, СТБ 34.101.3-2004);
- эксплуатационные документы;

- перечень взаимосвязанных с настоящим техническим регламентом государственных стандартов, требованиям которых соответствует средство защиты информации (при их применении изготовителем);
- протокол (протоколы) испытаний, проведенных в аккредитованных испытательных лабораториях;
- копии сертификатов на систему управления качеством и (или) систему управления безопасностью продукции (при наличии);
- заключает договор на проведение работ по сертификации продукции;
- предоставляет продукцию для проведения идентификации (схемы 1с, 2с, 3с, 4с) и отбора образцов для испытаний (схемы 1с, 3с);
- создает условия для проведения анализа состояния производства (схема 1с);
- заключает с аккредитованным органом по сертификации соглашение по сертификации (схемы 1с, 2с);
- создает условия для проведения инспекционного контроля за сертифицированной продукцией (схемы 1с, 2с);

7.3. аккредитованная испытательная лаборатория:

- заключает договор на проведение испытаний;
- проводит испытания продукции.

Аккредитованный орган по сертификации имеет право запросить дополнительную техническую (конструкторскую) документацию (тексты и описания программных средств, методики и программы испытаний, спецификации, сборочные чертежи, чертежи сборочных единиц и деталей, электрические схемы или иные документы, согласно которым изготавливается средство защиты информации), необходимую для подтверждения соответствия средства защиты информации требованиям информационной безопасности настоящего технического регламента.

8. Подтверждение соответствия средств защиты информации, указанных в пункте 4 настоящей статьи, проводится путем декларирования соответствия по одной из схем:

- при принятии заявителем декларации о соответствии на основании собственных доказательств:
  схема 1д – для серийно выпускаемой продукции;
  схема 2д – для партии продукции (единичного изделия);
- при принятии заявителем декларации о соответствии на основании собственных доказательств и доказательств, полученных с участием аккредитованного органа по сертификации и (или) аккредитованной испытательной лаборатории:
  схема 3д – для серийно выпускаемой продукции;
  схема 4д – для партии продукции (единичного изделия);
  схема 6д – для серийно выпускаемой продукции при наличии у изготовителя сертифицированных в Национальной системе подтверждения соответствия Республики Беларусь системы управления качеством и (или) системы управления безопасностью продукции.

Применяя указанные схемы:

8.1. аккредитованный орган по сертификации:

- заключает договор на проведение работ по подтверждению соответствия (регистрация декларации о соответствии);
- проводит анализ представленной заявителем декларации о соответствии;
- регистрирует декларацию о соответствии;

8.2. заявитель:

- формирует документы, подтверждающие соответствие продукции установленным требованиям и правомочность принятия декларации о соответствии;

- осуществляет контроль в процессе производства продукции (схемы 1д, 3д, 6д);
- проводит испытания продукции (схемы 1д, 2д, 6д);
- принимает декларацию о соответствии;
- предоставляет продукцию для испытаний (схемы 3д, 4д, 6д);
- подает заявление на регистрацию декларации о соответствии;
- заключает договор на проведение работ по подтверждению соответствия (регистрация декларации о соответствии) (схемы 1д, 2д, 3д, 4д, 6д) и испытаний (схемы 3д, 4д, 6д);

8.3. аккредитованная испытательная лаборатория:

- заключает договор на проведение испытаний (схемы 3д, 4д, 6д);
- проводит испытания продукции (схемы 3д, 4д, 6д).

9. Изготовитель осуществляет производственный контроль и принимает все необходимые меры, для того чтобы процесс производства обеспечивал соответствие средств защиты информации требованиям настоящего технического регламента.

Требования к процессам производства и контроля, а также результаты их контроля должны быть оформлены документально.

10. На территории Республики Беларусь должен храниться комплект документов на:

- средства защиты информации – у изготовителя (уполномоченного изготовителем лица) в течение не менее 10 лет со дня снятия с производства (прекращения производства) средств защиты информации;
- партию средств защиты информации – у импортера в течение не менее 10 лет со дня реализации последнего изделия из партии.

Комплект документов должен предоставляться органам государственного надзора по их требованию согласно законодательству.

Статья 7. Маркировка знаком соответствия

1. Средства защиты информации, соответствующие требованиям информационной безопасности и прошедшие процедуру подтверждения соответствия согласно статье 6 настоящего технического регламента, должны маркироваться знаком соответствия техническому регламенту согласно ТКП 5.1.08-2012.

2. Маркировка средств защиты информации знаком соответствия техническому регламенту осуществляется перед их выпуском в обращение на рынке.

3. Знак соответствия техническому регламенту наносится любым способом, обеспечивающим четкое и ясное изображение в течение всего срока службы средств защиты информации, на:

- каждую единицу технических и программно-аппаратных средств защиты информации;
- каждый носитель информации программных средств защиты информации;
- упаковку.

4. Маркировка средств защиты информации знаком соответствия техническому регламенту свидетельствует о соответствии данных средств требованиям всех технических регламентов, распространяющих на них свое действие и предусматривающих нанесение этого знака соответствия.

Статья 8. Государственный надзор за соблюдением настоящего технического регламента

Государственный надзор за соблюдением настоящего технического регламента осуществляется в порядке, установленном законодательством.

2. СОДЕРЖАНИЕ ОТЧЕТА

Цель работы.
Решение задания.
Ответы на контрольные задания.

3. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Определите область применения технического регламента.
2. Кто, согласно регламенту, является уполномоченным представителем изготовителя средств защиты информации?
3. Могут ли быть маркированы знаком соответствия средства защиты информации, которые не соответствуют требованиям настоящего технического регламента?
4. Как обеспечивается соответствие средств защиты информации настоящему техническому регламенту?
5. По каким критериям осуществляется оценка безопасности информационных технологий?

СПИСОК ИСТОЧНИКОВ

Основная литература:

1. ТР 2013/027/BY – Технический регламент Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность»

2. [Электрон, ресурс] – http://oac.gov.by Оперативно-аналитический центр при Президенте Республики Беларусь

3. [Электрон, ресурс] – http://www.tnpa.by Государственный комитет по стандартизации Республики Беларусь

4. СТБ 34.101.1-2004 (ИСО/МЭК 15408.1-99) Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

5. СТБ 34.101.2-2004 (ИСО/МЭК 15408.2-99) Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

6. СТБ 34.101.3-2004 (ИСО/МЭК 15408.3-99) Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности

7. СТБ ISO/IEC 27001 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

Дополнительная литература:

8. [Электрон, ресурс] – http://www.pravo.by

9. [Электрон, ресурс] – www.gosstandart.gov.by

10. [Электрон, ресурс] – http://www.iso.ch

ПРАКТИЧЕСКАЯ РАБОТА №2

ТЕМА: Правовое обеспечение информационной безопасности

ЦЕЛЬ РАБОТЫ: Изучить законы Республики Беларусь по определению правовых и организационных основ отнесения сведений к государственным секретам и их защите; государственное регулирование и управление в области информации, информатизации и защиты информации.

Результат обучения:

После успешного завершения занятия пользователь должен:

- знать законы Республики Беларусь по определению правовых и организационных основ отнесения сведений к государственным секретам и их защите.
- изучить возможности государственного регулирования и управления в области информации, информатизации и защиты информации в Республике Беларусь.

Используемая программа: Firefox, Internet Explorer, Opera и др.

План занятия:

1. Изучение кратких теоретических сведений.
2. Выполнение задания.
3. Оформление отчета.

1. КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Закон Республики Беларусь 19 июля 2010 г. №170-З «О Государственных Секретах»

Настоящий Закон 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.

ГЛАВА 1 ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Основные термины, используемые в настоящем Законе, и их определения

В настоящем Законе используются следующие основные термины и их определения:

государственные секреты (сведения, составляющие государственные секреты) – сведения, отнесенные в установленном порядке к государственным секретам, защищаемые государством в соответствии с настоящим Законом и другими актами законодательства Республики Беларусь;

гриф секретности – реквизит, проставляемый на носителе государственных секретов и (или) сопроводительной документации к нему, свидетельствующий о степени секретности содержащихся на этом носителе государственных секретов;

допуск к государственным секретам – право гражданина Республики Беларусь, иностранного гражданина, лица без гражданства (далее, если не указано иное, – гражданин) или государственного органа, иной организации на осуществление деятельности с использованием государственных секретов;

доступ к государственным секретам – ознакомление гражданина с государственными секретами или осуществление им иной деятельности с использованием государственных секретов;

носитель государственных секретов – материальный объект, на котором государственные секреты содержатся в виде символов, образов, сигналов и (или) технических решений и процессов, позволяющих их распознать и идентифицировать;

средства защиты государственных секретов – технические, программные, криптографические и другие средства, используемые для защиты государственных секретов, а также средства контроля эффективности защиты государственных секретов;

степень секретности – показатель важности государственных секретов, определяющий меры и средства защиты государственных секретов.

Статья 2. Законодательство Республики Беларусь о государственных секретах

Законодательство Республики Беларусь о государственных секретах основывается на Конституции Республики Беларусь и состоит из настоящего Закона, других актов законодательства Республики Беларусь, в том числе международных договоров Республики Беларусь о защите государственных секретов.

ГЛАВА 2 ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ И УПРАВЛЕНИЕ В СФЕРЕ ГОСУДАРСТВЕННЫХ СЕКРЕТОВ

Статья 3. Государственное регулирование и управление в сфере государственных секретов

Государственное регулирование и управление в сфере государственных секретов осуществляются Президентом Республики Беларусь, Советом Министров Республики Беларусь, а также Межведомственной комиссией по защите государственных секретов при Совете Безопасности Республики Беларусь, уполномоченным государственным органом по защите государственных секретов, органами государственной безопасности, Оперативно-аналитическим центром при Президенте Республики Беларусь.

Статья 4. Полномочия Президента Республики Беларусь

Президент Республики Беларусь в сфере государственных секретов:

определяет государственную политику;

утверждает государственные программы;

утверждает Положение о Межведомственной комиссии по защите государственных секретов при Совете Безопасности Республики Беларусь и ее состав;

создает, реорганизует и упраздняет уполномоченный государственный орган по защите государственных секретов;

утверждает перечень государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам, перечень сведений, подлежащих отнесению к государственным секретам;

ведет переговоры и подписывает межгосударственные договоры Республики Беларусь о защите государственных секретов;

принимает решения о передаче государственных секретов иностранным государствам, международным организациям, межгосударственным образованиям, если иное не установлено настоящим Законом;

устанавливает порядок предоставления допуска к государственным секретам иностранным гражданам и лицам без гражданства, а также гражданам Республики Беларусь, постоянно проживающим за пределами Республики Беларусь;

осуществляет иные полномочия в соответствии с настоящим Законом и другими законодательными актами Республики Беларусь.

Статья 5. Полномочия Совета Министров Республики Беларусь

Совет Министров Республики Беларусь в сфере государственных секретов: организует разработку проектов государственных программ, перечня государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам, перечня сведений, подлежащих отнесению к государственным секретам, и представляет их на утверждение Президенту Республики Беларусь, принимает меры по выполнению государственных программ;

организует разработку проектов актов законодательства Республики Беларусь, в том числе международных договоров Республики Беларусь о защите государственных секретов, принимает в пределах своей компетенции акты законодательства Республики Беларусь;

заключает межправительственные договоры Республики Беларусь о защите государственных секретов, принимает меры по реализации международных договоров Республики Беларусь о защите государственных секретов;

утверждает положение об экспертных комиссиях в сфере государственных секретов, перечень особо режимных и режимных объектов, положение об особо режимных и режимных объектах, порядок создания и деятельности подразделений по защите государственных секретов;

принимает решения о создании межведомственных экспертных комиссий в сфере государственных секретов;

устанавливает порядок определения тяжести последствий, которые наступили или могут наступить, размера вреда, который причинен или может быть причинен в результате разглашения или утраты государственных секретов;

устанавливает порядок предоставления гражданам допуска к государственным секретам, если иное не установлено настоящим Законом;

устанавливает с учетом положений настоящего Закона порядок осуществления гражданами доступа к государственным секретам;

устанавливает с учетом положений настоящего Закона порядок отнесения сведений к государственным секретам, засекречивания, рассекречивания, а также защиты государственных секретов;

устанавливает с учетом положений настоящего Закона порядок передачи государственных секретов государственным органам и иным организациям;

устанавливает с учетом положений настоящего Закона порядок передачи государственных секретов иностранным государствам, международным организациям, межгосударственным образованиям;

устанавливает размеры надбавок к тарифным ставкам (окладам) гражданам на период доступа к государственным секретам в зависимости от степени секретности, а также компенсационных выплат гражданам на период действия временного ограничения их права на выезд из Республики Беларусь, если они осведомлены о государственной тайне, и надбавок к тарифным ставкам (окладам) работникам подразделений по защите государственных секретов за стаж работы в указанных подразделениях, а также порядок их выплат;

определяет порядок материально-технического и финансового обеспечения деятельности в сфере государственных секретов;

осуществляет иные полномочия в соответствии с настоящим Законом и другими законодательными актами Республики Беларусь.

Статья 6. Полномочия Межведомственной комиссии по защите государственных секретов при Совете Безопасности Республики Беларусь

Межведомственная комиссия по защите государственных секретов при Совете Безопасности Республики Беларусь в сфере государственных секретов:

координирует деятельность государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам;

осуществляет подготовку предложений Президенту Республики Беларусь и Совету Безопасности Республики Беларусь о формировании государственной политики и совершенствовании защиты государственных секретов;

рассматривает проекты государственных программ, актов законодательства Республики Беларусь, в том числе международных договоров Республики Беларусь о защите государственных секретов;

осуществляет иные полномочия в соответствии с законодательными актами Республики Беларусь.

Статья 7. Полномочия уполномоченного государственного органа по защите государственных секретов

Уполномоченный государственный орган по защите государственных секретов в сфере государственных секретов:

координирует деятельность государственных органов и иных организаций по защите государственных секретов;

разрабатывает предложения о формировании государственной политики и совершенствовании защиты государственных секретов;

осуществляет государственный контроль;

разрабатывает проекты государственных программ, актов законодательства Республики Беларусь, в том числе международных договоров Республики Беларусь о защите государственных секретов, принимает в пределах своей компетенции акты законодательства Республики Беларусь;

проводит проверочные мероприятия в государственных органах и иных организациях в связи с предоставлением им допуска к государственным секретам;

устанавливает порядок выдачи разрешений на осуществление деятельности с использованием государственных секретов, выдает, приостанавливает, возобновляет и аннулирует разрешения на осуществление деятельности с использованием государственных секретов государственным органам и иным организациям, за исключением государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам;

согласовывает перечни сведений, подлежащих засекречиванию, номенклатуры должностей работников, подлежащих допуску к государственным секретам;

согласовывает предоставление гражданам допуска к государственным секретам, а также осуществление доступа к государственным секретам граждан, являющихся представителями иностранных государств, международных организаций, межгосударственных образований;

создает экспертные комиссии в сфере государственных секретов для рассмотрения материалов о возможности передачи государственных секретов иностранным государствам, международным организациям, межгосударственным образованиям, выносит заключения о возможности передачи государственных секретов иностранным государствам, международным организациям, межгосударственным образованиям;

осуществляет государственную регистрацию информационных систем, содержащих государственные секреты;

организует повышение квалификации, подготовку и переподготовку руководителей, ответственных за обеспечение защиты государственных секретов, и других работников государственных органов и иных организаций, осуществляющих деятельность с использованием государственных секретов;

оказывает методическую и практическую помощь государственным органам и иным организациям, осуществляющим деятельность с использованием государственных секретов, по вопросам защиты государственных секретов;

осуществляет иные полномочия в соответствии с настоящим Законом и другими актами законодательства Республики Беларусь.

Статья 8. Полномочия органов государственной безопасности

Органы государственной безопасности в сфере государственных секретов: организуют обеспечение государственных органов и иных организаций средствами шифрованной, других видов специальной связи, координируют их применение, осуществляют контроль за использованием указанных средств;

координируют применение государственными органами и иными организациями криптографических средств защиты государственных секретов, осуществляют контроль за их использованием;

осуществляют в пределах своих полномочий контроль за защитой государственных секретов, в том числе контроль при использовании криптографических средств защиты государственных секретов;

осуществляют подтверждение соответствия средств шифрованной, других видов специальной связи и криптографических средств защиты государственных секретов требованиям технических нормативных правовых актов Республики Беларусь в области технического нормирования и стандартизации и выдают сертификаты соответствия;

организуют применение технических мер защиты государственных секретов в своей деятельности, осуществляют контроль за их использованием;

разрабатывают проекты актов законодательства Республики Беларусь, в том числе технических нормативных правовых актов, принимают в пределах своей компетенции акты законодательства Республики Беларусь;

согласовывают создание, реорганизацию и ликвидацию государственными органами и иными организациями подразделений по защите государственных секретов, а также назначение на должности и освобождение от должностей руководителей этих подразделений;

проводят в пределах своей компетенции проверочные мероприятия в отношении граждан в связи с предоставлением им допуска к государственным секретам, осуществлением ими деятельности в сфере государственных секретов;

вносят предложения в государственные органы и иные организации, осуществляющие деятельность с использованием государственных секретов, о временном ограничении права граждан, осведомленных о государственной тайне, на выезд из Республики Беларусь;

вносят предписания в государственные органы и иные организации, осуществляющие деятельность с использованием государственных секретов, о прекращении допуска к государственным секретам граждан;

осуществляют иные полномочия в соответствии с настоящим Законом и другими актами законодательства Республики Беларусь.

Статья 9. Полномочия Оперативно-аналитического центра при Президенте Республики Беларусь

Оперативно-аналитический центр при Президенте Республики Беларусь в сфере государственных секретов:

координирует применение технических мер защиты государственных секретов в государственных органах и иных организациях, осуществляющих деятельность с использованием государственных секретов, за исключением применения технических мер защиты государственных секретов в системах шифрованной, других видов специальной связи и при использовании криптографических средств защиты государственных секретов, осуществляет контроль за применением указанных мер в порядке, установленном этим центром;

разрабатывает проекты актов законодательства Республики Беларусь о применении технических мер защиты государственных секретов, за исключением применения технических мер защиты государственных секретов в системах шифрованной, других видов специальной связи и при использовании криптографических средств защиты государственных секретов, а также проекты технических нормативных правовых актов Республики Беларусь в области технического нормирования и стандартизации средств защиты государственных секретов, за исключением систем шифрованной, других видов специальной связи и криптографических средств защиты государственных секретов, принимает в пределах своей компетенции акты законодательства Республики Беларусь;

осуществляет подтверждение соответствия средств защиты государственных секретов требованиям технических нормативных правовых актов Республики Беларусь в области технического нормирования и стандартизации, за исключением средств шифрованной, других видов специальной связи и криптографических средств защиты государственных секретов, и выдает сертификат соответствия;

осуществляет методическое руководство повышением квалификации, подготовкой и переподготовкой руководителей, ответственных за обеспечение защиты государственных секретов, и других работников государственных органов и иных организаций, осуществляющих деятельность с использованием государственных секретов, по применению технических мер защиты государственных секретов, определяет порядок их аттестации;

осуществляет иные полномочия в соответствии с актами законодательства Республики Беларусь.

ГЛАВА 3 ОСУЩЕСТВЛЕНИЕ ДЕЯТЕЛЬНОСТИ С ИСПОЛЬЗОВАНИЕМ ГОСУДАРСТВЕННЫХ СЕКРЕТОВ

Статья 10. Осуществление деятельности с использованием государственных секретов

Деятельность с использованием государственных секретов осуществляют государственные органы и иные организации, наделенные полномочием по отнесению сведений к государственным секретам, другие государственные органы, иные организации и граждане.

Условием осуществления деятельности с использованием государственных секретов является наличие у государственных органов, иных организаций и граждан допуска к государственным секретам, предоставленного в соответствии с настоящим Законом и другими актами законодательства Республики Беларусь.

Статья 11. Полномочия государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам

Государственные органы и иные организации, наделенные полномочием по отнесению сведений к государственным секретам, в сфере государственных секретов:

относят в сфере своей деятельности сведения к государственным секретам, разрабатывают и утверждают перечни сведений, подлежащих засекречиванию;

организуют и осуществляют в сфере своей деятельности защиту государственных секретов;

вносят в Совет Министров Республики Беларусь предложения о формировании перечня сведений, подлежащих отнесению к государственным секретам, перечня особо режимных и режимных объектов, а также предложения о создании межведомственных экспертных комиссий в сфере государственных секретов;

передают государственные секреты другим государственным органам и иным организациям;

принимают решения о передаче служебной тайны иностранным государствам, международным организациям, межгосударственным образованиям при наличии международного договора Республики Беларусь о защите государственных секретов;

осуществляют контроль за защитой государственных секретов в подчиненных организациях, а также в государственных органах и иных организациях, которым в связи с проведением работ с использованием государственных секретов передаются ими государственные секреты;

согласовывают создание, реорганизацию и ликвидацию подразделений по защите государственных секретов в подчиненных организациях, а также в других государственных органах и иных организациях, которым в связи с проведением работ с использованием государственных секретов передаются ими государственные секреты;

создают, реорганизуют и ликвидируют подразделения по защите государственных секретов, обеспечивают их функционирование;

определяют руководителей, ответственных за обеспечение защиты государственных секретов;

создают условия для осуществления деятельности с использованием государственных секретов;

разрабатывают и утверждают номенклатуры должностей работников, подлежащих допуску к государственным секретам;

принимают в пределах своей компетенции решения о создании экспертных комиссий в сфере государственных секретов;

обеспечивают повышение квалификации, подготовку и переподготовку руководителей, ответственных за обеспечение защиты государственных секретов, и других работников, осуществляющих деятельность с использованием государственных секретов;

осуществляют иные полномочия в соответствии с настоящим Законом и другими актами законодательства Республики Беларусь.

Статья 12. Полномочия других государственных органов и иных организаций

Другие государственные органы и иные организации, осуществляющие деятельность с использованием государственных секретов, в сфере государственных секретов:

организуют и осуществляют защиту государственных секретов, находящихся в их пользовании;

осуществляют полномочия, предусмотренные абзацами седьмым – четырнадцатым статьи 11 настоящего Закона;

вносят в государственные органы и иные организации, наделенные полномочием по отнесению сведений к государственным секретам, предложения о формировании перечня сведений, подлежащих отнесению к государственным секретам, перечней сведений, подлежащих засекречиванию, перечня особо режимных и режимных объектов, а также предложения о создании экспертных комиссий в сфере государственных секретов;

осуществляют иные полномочия в соответствии с настоящим Законом и другими актами законодательства Республики Беларусь.

Статья 13. Права и обязанности граждан

Граждане в сфере государственных секретов имеют право:

на осуществление деятельности с использованием государственных секретов с соблюдением требований, предусмотренных настоящим Законом и другими актами законодательства Республики Беларусь о государственных секретах;

на получение надбавок к тарифным ставкам (окладам) на период их доступа к государственным секретам в зависимости от степени секретности, а также компенсационных выплат на период действия временного ограничения их права на выезд из Республики Беларусь, если они осведомлены о государственной тайне, и надбавок к тарифным ставкам (окладам) за стаж работы в подразделениях по защите государственных секретов;

ознакомиться с законодательством Республики Беларусь о государственных секретах в необходимом объеме;

осуществлять иные права, предусмотренные настоящим Законом и другими актами законодательства Республики Беларусь.

Граждане обязаны выполнять требования, предусмотренные настоящим Законом и другими актами законодательства Республики Беларусь о государственных секретах.

ГЛАВА 4 СВЕДЕНИЯ, КОТОРЫЕ МОГУТ БЫТЬ ОТНЕСЕНЫ ЛИБО НЕ МОГУТ БЫТЬ ОТНЕСЕНЫ К ГОСУДАРСТВЕННЫМ СЕКРЕТАМ

Статья 14. Сведения, которые могут быть отнесены к государственным секретам

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 развертыванию 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.

Статья 15. Сведения, которые не могут быть отнесены 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.

ГЛАВА 5 КАТЕГОРИИ ГОСУДАРСТВЕННЫХ СЕКРЕТОВ. СТЕПЕНИ СЕКРЕТНОСТИ. ГРИФЫ СЕКРЕТНОСТИ

Статья 16. Категории государственных секретов

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.

Статья 17. Степени секретности

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".

Статья 18. Грифы секретности

На носителях государственных секретов и (или) сопроводительной документации к ним в зависимости от степени секретности государственных секретов проставляются следующие 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".

ГЛАВА 6 ОТНЕСЕНИЕ СВЕДЕНИЙ К ГОСУДАРСТВЕННЫМ СЕКРЕТАМ. ЗАСЕКРЕЧИВАНИЕ. РАССЕКРЕЧИВАНИЕ

Статья 19. Отнесение сведений к государственным секретам

Отнесение сведений к государственным секретам осуществляется посредством определения сведений, которые подлежат защите в соответствии с настоящим Законом и другими актами законодательства Республики Беларусь.

Отнесение сведений к государственным секретам осуществляется государственными органами и иными организациями, наделенными полномочием по отнесению сведений к государственным секретам, с учетом перечня сведений, подлежащих отнесению к государственным секретам.

Государственные органы и иные организации, наделенные полномочием по отнесению сведений к государственным секретам, в сфере своей деятельности разрабатывают и утверждают перечни сведений, подлежащих засекречиванию.

Сведения, полученные государственными органами и иными организациями, а также гражданами при осуществлении деятельности, не связанной с использованием государственных секретов, собственниками которых они являются, могут быть отнесены к государственным секретам после передачи их этими государственными органами и иными организациями, а также гражданами по договору государственному органу и иной организации, наделенным полномочием по отнесению сведений к государственным секретам. Договор о передаче таких сведений заключается в соответствии с Гражданским кодексом Республики Беларусь и должен содержать указание на условия передачи этих сведений.

До принятия решения об отнесении к государственным секретам сведений, указанных в части четвертой настоящей статьи, государственными органами и иными организациями, а также гражданами осуществляется их защита.

Статья 20. Определение и изменение степени секретности

Определение и изменение степени секретности осуществляются государственными органами и иными организациями, наделенными полномочием по отнесению сведений к государственным секретам, в сфере своей деятельности.

Статья 21. Засекречивание

Засекречивание осуществляется на основании перечня сведений, подлежащих засекречиванию, посредством установления ограничений на распространение и (или) предоставление сведений и применения иных мер защиты в соответствии с настоящим Законом и другими актами законодательства Республики Беларусь.

При засекречивании на носителе государственных секретов и (или) сопроводительной документации к нему проставляется гриф секретности.

Статья 22. Срок засекречивания, изменение срока засекречивания

Для государственных секретов, как правило, устанавливаются следующие сроки засекречивания:

для государственной тайны – до тридцати лет;

для служебной тайны – до десяти лет.

Срок засекречивания исчисляется с даты засекречивания.

Изменение срока засекречивания осуществляется на основании решений государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам.

Статья 23. Рассекречивание

Рассекречивание осуществляется посредством снятия ограничений на распространение и (или) предоставление государственных секретов и прекращения иных мер защиты.

Рассекречивание осуществляется на основании решений государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам.

При рассекречивании на носителях государственных секретов и (или) сопроводительной документации к ним аннулируется гриф секретности.

ГЛАВА 7 ПРАВО СОБСТВЕННОСТИ НА ГОСУДАРСТВЕННЫЕ СЕКРЕТЫ. ВЛАДЕНИЕ, ПОЛЬЗОВАНИЕ И РАСПОРЯЖЕНИЕ ГОСУДАРСТВЕННЫМИ СЕКРЕТАМИ

Статья 24. Право собственности на государственные секреты

Государственные секреты являются собственностью Республики Беларусь.

Статья 25. Владение, пользование и распоряжение государственными секретами

Государственные органы и иные организации, наделенные полномочием по отнесению сведений к государственным секретам, в сфере своей деятельности осуществляют владение, пользование и распоряжение государственными секретами в соответствии с актами законодательства Республики Беларусь.

Другие государственные органы и иные организации, осуществляющие деятельность с использованием государственных секретов, реализуют право пользования государственными секретами, а также в пределах полномочий, предоставленных им государственными органами и иными организациями, наделенными полномочием по отнесению сведений к государственным секретам, распоряжаются государственными секретами.

Статья 26. Передача государственных секретов государственным органам и иным организациям

Государственные секреты передаются государственным органам и иным организациям в целях осуществления ими своих полномочий либо в связи с проведением работ с использованием государственных секретов в объеме, необходимом для осуществления этих полномочий либо проведения таких работ.

Передача государственных секретов государственным органам и иным организациям осуществляется на основании решений государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам.

Статья 27. Передача государственных секретов иностранным государствам, международным организациям, межгосударственным образованиям

Передача государственных секретов иностранным государствам, международным организациям, межгосударственным образованиям осуществляется на основании решений Президента Республики Беларусь или руководителей государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам, в пределах их компетенции с учетом заключения уполномоченного государственного органа по защите государственных секретов о возможности их передачи.

Решение о передаче государственных секретов иностранным государствам, международным организациям, межгосударственным образованиям принимается Президентом Республики Беларусь при наличии обязательства иностранного государства, международной организации, межгосударственного образования о защите государственных секретов.

Решение о передаче служебной тайны иностранным государствам, международным организациям, межгосударственным образованиям принимается руководителями государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам, при наличии международного договора **Республики** Беларусь о защите государственных секретов.

ГЛАВА 8 ЗАЩИТА ГОСУДАРСТВЕННЫХ СЕКРЕТОВ

Статья 28. Организация защиты государственных секретов в государственных органах и иных организациях

Организация защиты государственных секретов в государственных органах и иных организациях возлагается на их руководителей.

Защита государственных секретов осуществляется посредством применения правовых, организационных, технических мер, в том числе посредством использования сертифицированных средств защиты государственных секретов, и иных мер в соответствии с настоящим Законом и другими актами законодательства Республики Беларусь в целях

предотвращения тяжких последствий или существенного вреда национальной безопасности Республики Беларусь.

В государственных органах и иных организациях, наделенных полномочием по отнесению сведений к государственным секретам, должны быть созданы подразделения по защите государственных секретов.

Другие государственные органы и иные организации по решению их руководителей создают подразделения по защите государственных секретов или заключают договор об оказании услуг по защите государственных секретов с государственным органом и иной организацией, имеющими подразделение по защите государственных секретов, по согласованию с государственным органом и иной организацией, которые передают им государственные секреты.

Государственные органы и иные организации в случае их реорганизации или ликвидации, а также прекращения деятельности с использованием государственных секретов обязаны в соответствии с настоящим Законом и другими актами законодательства Республики Беларусь принять меры по защите находящихся у них государственных секретов.

Статья 29. Защита государственных секретов иностранных государств, международных организаций, межгосударственных образований

Защита государственных секретов иностранных государств, международных организаций, межгосударственных образований, переданных Республике Беларусь на основании международных договоров Республики Беларусь либо в связи с ее членством в этих международных организациях, межгосударственных образованиях, а также сведений, образовавшихся при их использовании, осуществляется в соответствии с настоящим Законом, другими актами законодательства Республики Беларусь, в том числе международными договорами Республики Беларусь о защите государственных секретов, с учетом требований иностранных государств, международных организаций, межгосударственных образований, передавших государственные секреты.

ГЛАВА 9 ДОПУСК К ГОСУДАРСТВЕННЫМ СЕКРЕТАМ. ДОСТУП К ГОСУДАРСТВЕННЫМ СЕКРЕТАМ

Статья 30. Условия предоставления допуска к государственным секретам государственным органам и иным организациям

Допуск к государственным секретам государственным органам и иным организациям предоставляется при соблюдении ими законодательства Республики Беларусь о государственных секретах, а также если:

в их структуре имеется подразделение по защите государственных секретов, состоящее из работников, количество и уровень квалификации которых достаточны для защиты государственных секретов, или ими заключен договор об оказании услуг по защите государственных секретов с государственным органом и иной организацией, имеющими подразделение по защите государственных секретов;

разработана и утверждена номенклатура должностей работников, подлежащих допуску к государственным секретам;

их руководители, ответственные за обеспечение защиты государственных секретов, имеют допуск к государственным секретам;

приняты иные меры защиты государственных секретов, предусмотренные законодательством Республики Беларусь о государственных секретах.

Статья 31. Допуск к государственным секретам государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам

Допуск к государственным секретам государственным органам и иным организациям, наделенным полномочием по отнесению сведений к государственным секретам, предоставляется на основании включения их в перечень государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам, утвержденный Президентом Республики Беларусь.

Государственные органы и иные организации, наделенные полномочием по отнесению сведений к государственным секретам, осуществляют деятельность с использованием государственных секретов при наличии в их структуре подразделения по защите государственных секретов и выполнении условий, предусмотренных абзацами первым, третьим – пятым статьи 30 настоящего Закона. Информация о состоянии защиты государственных секретов в государственных органах и иных организациях, наделенных полномочием по отнесению сведений к государственным секретам, учитывается при проведении в соответствии с актами законодательства Республики Беларусь аттестации их руководителей.

Статья 32. Допуск к государственным секретам других государственных органов и иных организаций

Допуск к государственным секретам другим государственным органам и иным организациям предоставляется на основании разрешения на осуществление деятельности с использованием государственных секретов, выданного уполномоченным государственным органом по защите государственных секретов по результатам проверочных мероприятий.

Разрешение на осуществление деятельности с использованием государственных секретов выдается после выполнения другими государственными органами и иными организациями условий, предусмотренных статьей 30 настоящего Закона, и аттестации их руководителей, ответственных за обеспечение защиты государственных секретов.

Статья 33. Условия предоставления гражданам допуска к государственным секретам

Допуск к государственным секретам гражданам предоставляется, если:

граждане ознакомлены с правами и обязанностями, предусмотренными настоящим Законом 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.

Допуск к государственным секретам гражданам Республики Беларусь, указанным в статье 35 настоящего Закона, предоставляется без согласования с уполномоченным государственным органом по защите государственных секретов и проведения в отношении

их проверочных мероприятий в связи с предоставлением им допуска к государственным секретам.

Допуск к государственным секретам гражданам, оказывающим на конфиденциальной основе содействие органам, осуществляющим разведывательную, контрразведывательную и оперативно-розыскную деятельность, а также гражданам Республики Беларусь, являющимся штатными негласными сотрудниками указанных органов, предоставляется без согласования с уполномоченным государственным органом по защите государственных секретов.

Гражданам, достигшим шестнадцатилетнего возраста, но не достигшим восемнадцатилетнего возраста, предоставляется допуск к служебной тайне.

Проверочные мероприятия в отношении граждан в связи с предоставлением им допуска к государственным секретам проводятся органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность, в пределах их компетенции.

Статья 34. Допуск к государственным секретам граждан

Допуск к государственным секретам предоставляется:

гражданам Республики Беларусь, постоянно проживающим в Республике Беларусь, являющимся работниками государственных органов и иных организаций, осуществляющих деятельность с использованием государственных секретов, – на основании решений руководителей государственных органов и иных организаций, принимаемых ими с учетом обязанностей, исполняемых работниками по месту работы (службы);

гражданам Республики Беларусь, постоянно проживающим в Республике Беларусь, не являющимся работниками государственных органов и иных организаций, осуществляющих деятельность с использованием государственных секретов, – на основании решений руководителей государственных органов и иных организаций о привлечении их к проведению работ с использованием государственных секретов;

гражданам Республики Беларусь, указанным в статье 35 настоящего Закона, – на основании решений об избрании (назначении) их на соответствующие должности, о признании их полномочий;

участникам уголовного, гражданского, хозяйственного, административного процесса, не имеющим допуска к государственным секретам, – на основании решений органов, ведущих соответственно уголовный, гражданский, хозяйственный или административный процесс;

иностранным гражданам и лицам без гражданства, а также гражданам Республики Беларусь, постоянно проживающим за пределами Республики Беларусь (за исключением граждан, являющихся представителями иностранных государств, международных организаций, межгосударственных образований, участвующих в реализации заключенных договоров (контрактов), предусматривающих использование государственных секретов), – на основании решений об использовании в интересах Республики Беларусь их профессиональных навыков и квалификации, принимаемых с учетом заключения уполномоченного государственного органа по защите государственных секретов о предоставлении им допуска к государственным секретам;

гражданам, оказывающим на конфиденциальной основе содействие органам, осуществляющим разведывательную, контрразведывательную и оперативно-розыскную деятельность, а также гражданам Республики Беларусь, являющимся штатными негласными сотрудниками указанных органов, – на основании решений, принимаемых органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность.

Решение о предоставлении гражданам допуска к государственным секретам принимается в соответствии с настоящим Законом и другими актами законодательства Республики Беларусь.

Статья 35. Допуск к государственным секретам граждан Республики Беларусь в связи с их избранием (назначением) на должность

Допуск к государственным секретам в связи с избранием (назначением) на должность предоставляется:

Президенту Республики Беларусь – с момента вступления его в должность;

Премьер-министру Республики Беларусь – с даты назначения его на должность;

депутатам Палаты представителей, членам Совета Республики Национального собрания Республики Беларусь, депутатам местных Советов депутатов – с даты признания их полномочий;

судьям – с даты назначения (избрания) их на должность.

Статья 36. Формы допуска к государственным секретам

В зависимости от степени секретности устанавливаются три формы допуска к государственным секретам:

форма №1 – форма допуска к государственной тайне, имеющей степень секретности "Особой важности";

форма №2 – форма допуска к государственной тайне, имеющей степень секретности "Совершенно секретно";

форма №3 – форма допуска к служебной тайне, имеющей степень секретности "Секретно".

Статья 37. Основания для отказа в предоставлении гражданам допуска к государственным секретам

Основаниями для отказа в предоставлении гражданину допуска к государственным секретам являются:

невыполнение условий предоставления допуска к государственным секретам;

признание судом гражданина недееспособным;

наличие у гражданина заболевания, препятствующего работе с государственными секретами, согласно перечню, утвержденному Министерством здравоохранения Республики Беларусь.

В предоставлении гражданину допуска к государственным секретам может быть отказано при:

возбуждении в отношении этого гражданина уголовного дела либо привлечении его в качестве подозреваемого или обвиняемого по уголовному делу, возбужденному в отношении других граждан, либо по факту совершения преступления;

наличии в уголовном, гражданском, хозяйственном или административном процессе дела, связанного с нарушением этим гражданином законодательства Республики Беларусь о государственных секретах;

наличии у гражданина неснятой или непогашенной судимости за совершение умышленного преступления;

оформлении гражданином документов для постоянного проживания за пределами Республики Беларусь;

представлении гражданином заведомо ложных его персональных данных.

Решение об отказе в предоставлении гражданам допуска к государственным секретам принимается в соответствии с настоящим Законом и другими актами законодательства Республики Беларусь и может быть обжаловано в вышестоящий государственный орган (вышестоящую организацию) и (или) в суд.

Статья 38. Прекращение допуска к государственным секретам граждан

Допуск к государственным секретам граждан прекращается в случае:

прекращения гражданами трудовых отношений с государственными органами и иными организациями, осуществляющими деятельность с использованием государственных секретов;

завершения участия граждан в проведении работ с использованием государственных секретов либо прекращения проведения таких работ;

прекращения полномочий граждан Республики Беларусь, указанных в статье 35 настоящего Закона;

завершения участия граждан в уголовном, гражданском, хозяйственном или административном процессе, которым допуск к государственным секретам был предоставлен по решению органа, ведущего уголовный, гражданский, хозяйственный или административный процесс;

завершения использования в интересах Республики Беларусь профессиональных навыков и квалификации граждан;

завершения оказания гражданами на конфиденциальной основе содействия органам, осуществляющим разведывательную, контрразведывательную и оперативно-розыскную деятельность, или исполнения обязанностей штатного негласного сотрудника указанных органов;

исключения из обязанностей, исполняемых гражданами по месту работы (службы) либо в ходе проведения работ с использованием государственных секретов, осуществления деятельности с использованием государственных секретов;

возникновения оснований, предусмотренных частью первой статьи 37 настоящего Закона;

внесения органом государственной безопасности в государственные органы и иные организации, осуществляющие деятельность с использованием государственных секретов, предписаний о прекращении допуска к государственным секретам граждан.

Прекращение допуска к государственным секретам граждан не освобождает их от соблюдения законодательства Республики Беларусь о государственных секретах, в том числе от возможного временного ограничения их права на выезд из Республики Беларусь, если они осведомлены о государственной тайне.

Решение о прекращении допуска к государственным секретам принимается в соответствии с настоящим Законом и другими актами законодательства Республики Беларусь и может быть обжаловано в вышестоящий государственный орган (вышестоящую организацию) и (или) в суд.

Статья 39. Доступ к государственным секретам граждан

Доступ к государственным секретам осуществляется гражданами на основании предоставленного им допуска к государственным секретам после их ознакомления в необходимом объеме с законодательством Республики Беларусь о государственных секретах.

Руководители государственных органов и иных организаций, осуществляющих деятельность с использованием государственных секретов, создают условия для осуществления гражданами доступа к государственным секретам, при которых граждане будут иметь доступ только к тем государственным секретам и в таком объеме, которые необходимы им для исполнения их обязанностей.

Доступ к государственным секретам, имеющим степени секретности "Особой важности", "Совершенно секретно" и "Секретно", осуществляется при наличии допуска к государственным секретам формы N 1.

Доступ к государственным секретам, имеющим степени секретности "Совершенно секретно" и "Секретно", осуществляется при наличии допуска к государственным секретам формы №2.

Доступ к государственным секретам, имеющим степень секретности "Секретно", осуществляется при наличии допуска к государственным секретам формы N 3.

Доступ к государственным секретам осуществляется:

гражданами Республики Беларусь, постоянно проживающими в Республике Беларусь, – в период исполнения ими обязанностей по месту работы (службы) либо в связи с привлечением их к проведению работ с использованием государственных секретов;

гражданами Республики Беларусь, указанными в статье 35 настоящего Закона, – в период осуществления ими полномочий в связи с избранием (назначением) их на соответствующие должности;

участниками уголовного, гражданского, хозяйственного или административного процесса – в соответствии с процессуальным законодательством Республики Беларусь;

иностранными гражданами и лицами без гражданства, а также гражданами Республики Беларусь, постоянно проживающими за пределами Республики Беларусь (за исключением граждан, являющихся представителями иностранных государств, международных организаций, межгосударственных образований, участвующих в реализации заключенных договоров (контрактов), предусматривающих использование государственных секретов), – в период использования в интересах Республики Беларусь их профессиональных навыков и квалификации;

гражданами, являющимися представителями иностранных государств, международных организаций, межгосударственных образований, участвующими в реализации заключенных договоров (контрактов), предусматривающих использование государственных секретов, при наличии международных договоров Республики Беларусь о защите государственных секретов и по согласованию с уполномоченным государственным органом по защите государственных секретов – в период их участия в реализации заключенных договоров (контрактов), предусматривающих использование государственных секретов;

гражданами, оказывающими на конфиденциальной основе содействие органам, осуществляющим разведывательную, контрразведывательную и оперативно-розыскную деятельность, а также гражданами Республики Беларусь, являющимися штатными негласными сотрудниками указанных органов, – в период оказания ими содействия на конфиденциальной основе или исполнения обязанностей штатного негласного сотрудника этих органов.

ГЛАВА 10 ЗАЩИТА ПРАВ И ЗАКОННЫХ ИНТЕРЕСОВ ГОСУДАРСТВЕННЫХ ОРГАНОВ, ИНЫХ ОРГАНИЗАЦИЙ И ГРАЖДАН В СФЕРЕ ГОСУДАРСТВЕННЫХ СЕКРЕТОВ

Статья 40. Защита прав и законных интересов государственных органов, иных организаций и граждан в сфере государственных секретов

Защита прав и законных интересов государственных органов, иных организаций и граждан в сфере государственных секретов осуществляется в соответствии с настоящим Законом и другими законодательными актами Республики Беларусь.

Вред, причиненный в результате нарушения законодательства Республики Беларусь о государственных секретах, подлежит возмещению в порядке, установленном актами законодательства Республики Беларусь.

Статья 41. Временное ограничение прав граждан

Граждане временно ограничиваются в праве на неприкосновенность личной жизни в период проведения в отношении их проверочных мероприятий в связи с предоставлением им допуска к государственным секретам.

Граждане, осведомленные о государственной тайне, могут быть временно ограничены в праве на выезд из Республики Беларусь в соответствии с законодательными актами Республики Беларусь.

Статья 42. Предоставление гражданам надбавок и компенсационных выплат

Гражданам, осуществляющим либо осуществлявшим доступ к государственным секретам, устанавливаются надбавки к тарифным ставкам (окладам) на период их доступа к государственным секретам в зависимости от степени секретности, а также компенсационные выплаты на период действия временного ограничения их права на выезд из Республики Беларусь, если они осведомлены о государственной тайне.

Работникам подразделений по защите государственных секретов в государственных органах и иных организациях, осуществляющих деятельность с использованием государственных секретов, дополнительно к установленным частью первой настоящей статьи надбавкам и компенсационным выплатам устанавливаются за стаж работы в указанных подразделениях надбавки к тарифным ставкам (окладам).

ГЛАВА 11 НАДЗОР, КОНТРОЛЬ И ОТВЕТСТВЕННОСТЬ В СФЕРЕ ГОСУДАРСТВЕННЫХ СЕКРЕТОВ. ФИНАНСИРОВАНИЕ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ГОСУДАРСТВЕННЫХ СЕКРЕТОВ

Статья 43. Надзор за исполнением законодательства Республики Беларусь о государственных секретах

Надзор за точным и единообразным исполнением законодательства Республики Беларусь о государственных секретах осуществляют Генеральный прокурор Республики Беларусь и подчиненные ему прокуроры в пределах предоставленных им полномочий.

Статья 44. Государственный контроль в сфере государственных секретов

Государственный контроль в сфере государственных секретов осуществляется уполномоченным государственным органом по защите государственных секретов в порядке, установленном Президентом Республики Беларусь.

Статья 45. Контроль за защитой государственных секретов

Контроль за защитой государственных секретов в пределах полномочий осуществляется органами государственной безопасности, государственными органами и иными организациями, наделенными полномочием по отнесению сведений к государственным секретам, другими государственными органами и иными организациями, осуществляющими деятельность с использованием государственных секретов, в порядке, установленном Советом Министров Республики Беларусь.

Статья 46. Ответственность в сфере государственных секретов

Нарушение законодательства Республики Беларусь о государственных секретах влечет ответственность, установленную законодательными актами Республики Беларусь.

Ответственность за организацию защиты государственных секретов в государственных органах и иных организациях, осуществляющих деятельность с использованием государственных секретов, возлагается на их руководителей.

Статья 47. Финансирование мероприятий по защите государственных секретов

Финансирование мероприятий по защите государственных секретов осуществляется за счет средств республиканского и местных бюджетов, а также иных источников, не запрещенных актами законодательства Республики Беларусь.

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

ГЛАВА 1 ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Основные термины, применяемые в настоящем Законе, и их определения

В настоящем Законе применяются следующие основные термины и их определения:

база данных – совокупность структурированной и взаимосвязанной информации, организованной по определенным правилам на материальных носителях;

банк данных – организационно-техническая система, включающая одну или несколько баз данных и систему управления ими;

владелец программно-технических средств, информационных ресурсов, информационных систем и информационных сетей – субъект информационных отношений, реализующий права владения, пользования и распоряжения программно-техническими средствами, информационными ресурсами, информационными системами и информационными сетями в пределах и порядке, определенных их собственником в соответствии с законодательством Республики Беларусь;

государственная информационная система – информационная система, создаваемая и (или) приобретаемая за счет средств республиканского или местных бюджетов, государственных внебюджетных фондов, а также средств государственных юридических лиц;

государственный информационный ресурс – информационный ресурс, формируемый или приобретаемый за счет средств республиканского или местных бюджетов, государственных внебюджетных фондов, а также средств государственных юридических лиц;

документированная информация – информация, зафиксированная на материальном носителе с реквизитами, позволяющими ее идентифицировать;

доступ к информации – возможность получения информации и пользования ею;

доступ к информационной системе и (или) информационной сети – возможность использования информационной системы и (или) информационной сети;

защита информации – комплекс правовых, организационных и технических мер, направленных на обеспечение целостности (неизменности), конфиденциальности, доступности и сохранности информации;

информатизация – организационный, социально-экономический и научно-технический процесс, обеспечивающий условия для формирования и использования информационных ресурсов и реализации информационных отношений;

информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

информационная сеть – совокупность информационных систем либо комплексов программно-технических средств информационной системы, взаимодействующих посредством сетей электросвязи;

информационная система – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств;

информационная технология – совокупность процессов, методов осуществления поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией и защиты информации;

информационная услуга – деятельность по осуществлению поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также защиты информации;

информационные отношения – отношения, возникающие при поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, пользовании информацией, защите информации, а также при применении информационных технологий;

информационный посредник – субъект информационных отношений, предоставляющий информационные услуги обладателям и (или) пользователям информации;

информационный ресурс – организованная совокупность документированной информации, включающая базы данных, другие совокупности взаимосвязанной информации в информационных системах;

комплекс программно-технических средств – совокупность программных и технических средств, обеспечивающих осуществление информационных отношений с помощью информационных технологий;

конфиденциальность информации – требование не допускать распространения и (или) предоставления информации без согласия ее обладателя или иного основания, предусмотренного законодательными актами Республики Беларусь; обладатель информации – субъект информационных отношений, получивший права обладателя информации по основаниям, установленным актами законодательства Республики Беларусь, или по договору;

оператор информационной системы – субъект информационных отношений, осуществляющий эксплуатацию информационной системы и (или) оказывающий посредством ее информационные услуги;

пользователь информации – субъект информационных отношений, получающий, распространяющий и (или) предоставляющий информацию, реализующий право на пользование ею;

пользователь информационной системы и (или) информационной сети – субъект информационных отношений, получивший доступ к информационной системе и (или) информационной сети и пользующийся ими;

предоставление информации – действия, направленные на ознакомление с информацией определенного круга лиц;

распространение информации – действия, направленные на ознакомление с информацией неопределенного круга лиц;

собственник программно-технических средств, информационных ресурсов, информационных систем и информационных сетей – субъект информационных отношений, реализующий права владения, пользования и распоряжения программно-техническими средствами, информационными ресурсами, информационными системами и информационными сетями.

Статья 2. Сфера действия настоящего Закона

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.

Законодательством Республики Беларусь могут быть установлены особенности правового регулирования информационных отношений, связанных со сведениями,

составляющими государственные секреты, с персональными данными, рекламой, научно-технической, статистической, правовой и иной информацией.

Действие настоящего Закона не распространяется на общественные отношения, связанные с деятельностью средств массовой информации и охраной информации, являющейся объектом интеллектуальной собственности.

Статья 3. Законодательство об информации, информатизации и защите информации

Законодательство об информации, информатизации и защите информации основывается на Конституции Республики Беларусь и состоит из настоящего Закона, актов Президента Республики Беларусь, иных актов законодательства Республики Беларусь.

Если международным договором Республики Беларусь установлены иные правила, чем те, которые предусмотрены настоящим Законом, то применяются правила международного договора.

Статья 4. Принципы правового регулирования информационных отношений

Правовое регулирование информационных отношений осуществляется на основе следующих принципов:

свободы поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией;

установления ограничений распространения и (или) предоставления информации только законодательными актами Республики Беларусь;

своевременности предоставления, объективности, полноты и достоверности информации;

защиты информации о частной жизни физического лица и персональных данных;

обеспечения безопасности личности, общества и государства при пользовании информацией и применении информационных технологий;

обязательности применения определенных информационных технологий для создания и эксплуатации информационных систем и информационных сетей в случаях, установленных законодательством Республики Беларусь.

Статья 5. Субъекты информационных отношений

Субъектами информационных отношений могут являться:

Республика Беларусь, административно-территориальные единицы Республики Беларусь;

государственные органы, другие государственные организации (далее – государственные органы);

иные юридические лица, организации, не являющиеся юридическими лицами (далее – юридические лица);

физические лица, в том числе индивидуальные предприниматели (далее – физические лица);

иностранные государства, международные организации.

Субъекты информационных отношений в соответствии с настоящим Законом могут выступать в качестве:

обладателей информации;

пользователей информации, информационных систем и (или) информационных сетей;

собственников и владельцев программно-технических средств, информационных ресурсов, информационных систем и информационных сетей;

информационных посредников;

операторов информационных систем.

Статья 6. Право на информацию

Государственные органы, физические и юридические лица вправе осуществлять поиск, получение, передачу, сбор, обработку, накопление, хранение, распространение и (или) предоставление информации, пользование информацией в соответствии с настоящим Законом и иными актами законодательства Республики Беларусь.

Государственные органы, общественные объединения, должностные лица обязаны предоставлять гражданам Республики Беларусь возможность ознакомления с информацией, затрагивающей их права и законные интересы, в порядке, установленном настоящим Законом и иными актами законодательства Республики Беларусь.

Гражданам Республики Беларусь гарантируется право на получение, хранение и распространение полной, достоверной и своевременной информации о деятельности государственных органов, общественных объединений, о политической, экономической, культурной и международной жизни, состоянии окружающей среды в порядке, установленном настоящим Законом и иными актами законодательства Республики Беларусь.

Право на информацию не может быть использовано для пропаганды войны или экстремистской деятельности, а также для совершения иных противоправных деяний.

ГЛАВА 2 ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ И УПРАВЛЕНИЕ В ОБЛАСТИ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЫ ИНФОРМАЦИИ

Статья 7. Государственное регулирование в области информации, информатизации и защиты информации

Государственное регулирование в области информации, информатизации и защиты информации включает:

обеспечение условий для реализации и защиты прав государственных органов, физических и юридических лиц;

создание системы информационной поддержки решения задач социально-экономического и научно-технического развития Республики Беларусь;

создание условий для развития и использования информационных технологий, информационных систем и информационных сетей на основе единых принципов технического нормирования и стандартизации, оценки соответствия требованиям технических нормативных правовых актов в области технического нормирования и стандартизации;

формирование и осуществление единой научной, научно-технической, промышленной и инновационной политики в области информации, информатизации и защиты информации с учетом имеющегося научно-производственного потенциала и современного мирового уровня развития информационных технологий;

создание и совершенствование системы привлечения инвестиций и механизма стимулирования разработки и реализации проектов в области информации, информатизации и защиты информации;

содействие развитию рынка информационных технологий и информационных услуг, обеспечение условий для формирования и развития всех видов информационных ресурсов, информационных систем и информационных сетей;

обеспечение условий для участия Республики Беларусь, административно-территориальных единиц Республики Беларусь, государственных органов, физических и юридических лиц в международном сотрудничестве, включая взаимодействие с международными организациями, обеспечение выполнения обязательств по международным договорам Республики Беларусь;

разработку и обеспечение реализации целевых программ создания информационных систем, применения информационных технологий;

совершенствование законодательства Республики Беларусь об информации, информатизации и защите информации;

иное государственное регулирование.

Статья 8. Осуществление государственного регулирования и управления в области информации, информатизации и защиты информации

Государственное регулирование и управление в области информации, информатизации и защиты информации осуществляются Президентом Республики Беларусь, Советом Министров Республики Беларусь, Национальной академией наук Беларуси, Оперативно-аналитическим центром при Президенте Республики Беларусь, Министерством связи и информатизации Республики Беларусь, иными государственными органами в пределах их компетенции.

Статья 9. Полномочия Президента Республики Беларусь в области информации, информатизации и защиты информации

Президент Республики Беларусь в соответствии с Конституцией Республики Беларусь, настоящим Законом и иными законодательными актами Республики Беларусь определяет единую государственную политику и осуществляет иное государственное регулирование в области информации, информатизации и защиты информации.

Статья 10. Полномочия Совета Министров Республики Беларусь в области информации, информатизации и защиты информации

Совет Министров Республики Беларусь в области информации, информатизации и защиты информации:

обеспечивает проведение единой государственной политики;

координирует, направляет и контролирует работу республиканских органов государственного управления и иных государственных организаций, подчиненных Правительству Республики Беларусь;

утверждает государственные программы, если иное не предусмотрено законодательными актами Республики Беларусь, и обеспечивает их реализацию;

осуществляет иные полномочия, возложенные на него Конституцией Республики Беларусь, настоящим Законом, иными законами Республики Беларусь и актами Президента Республики Беларусь.

Статья 11. Полномочия Национальной академии наук Беларуси в области информации, информатизации и защиты информации

Национальная академия наук Беларуси в области информации, информатизации и защиты информации:

осуществляет научно-методическое обеспечение развития информатизации, реализации государственных программ;

участвует в разработке проектов нормативных правовых актов;

осуществляет иные полномочия в соответствии с настоящим Законом и иными законодательными актами Республики Беларусь.

Статья 12. Полномочия Оперативно-аналитического центра при Президенте Республики Беларусь в области защиты информации

Оперативно-аналитический центр при Президенте Республики Беларусь в области защиты информации:

определяет приоритетные направления технической защиты информации, содержащей сведения, составляющие государственные секреты, или иные сведения, охраняемые в соответствии с законодательством Республики Беларусь;

координирует деятельность по технической защите информации;

осуществляет в пределах своих полномочий контроль за деятельностью по обеспечению технической защиты информации;

участвует в разработке проектов нормативных правовых актов в области технической защиты информации;

осуществляет иные полномочия в соответствии с настоящим Законом и иными законодательными актами Республики Беларусь.

Статья 13. Полномочия Министерства связи и информатизации Республики Беларусь в области информатизации

Министерство связи и информатизации Республики Беларусь в области информатизации:

реализует единую государственную политику;

разрабатывает и реализует государственные программы;

участвует в разработке проектов нормативных правовых актов;

координирует работу по формированию и государственной регистрации информационных ресурсов;

устанавливает требования совместимости информационных ресурсов, информационных систем и информационных сетей;

разрабатывает и утверждает правила эксплуатации и взаимодействия информационных ресурсов, информационных систем и информационных сетей;

организует работы по техническому нормированию и стандартизации, подтверждению соответствия создания, использования и эксплуатации информационных ресурсов, информационных систем и информационных сетей требованиям технических нормативных правовых актов в области технического нормирования и стандартизации;

стимулирует создание информационных технологий, информационных систем и информационных сетей;

осуществляет международное сотрудничество, включая взаимодействие с международными организациями, обеспечение выполнения обязательств по международным договорам Республики Беларусь;

осуществляет иные полномочия в соответствии с настоящим Законом и иными актами законодательства Республики Беларусь.

Статья 14. Полномочия иных государственных органов в области информации, информатизации и защиты информации

Иные государственные органы в пределах своих полномочий в области информации, информатизации и защиты информации:

участвуют в реализации единой государственной политики;

формируют и используют информационные ресурсы;

создают и развивают информационные системы и информационные сети, обеспечивают их совместимость и взаимодействие в информационном пространстве Республики Беларусь;

осуществляют техническое нормирование и стандартизацию в области информационных технологий, информационных ресурсов, информационных систем и информационных сетей;

осуществляют подтверждение соответствия информационных технологий, информационных ресурсов, информационных систем и информационных сетей требованиям технических нормативных правовых актов в области технического нормирования и стандартизации;

осуществляют иные полномочия в соответствии с настоящим Законом и иными актами законодательства Республики Беларусь.

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.

Статья 16. Общедоступная информация

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

Не могут быть ограничены доступ к информации, распространение и (или) предоставление информации:

о правах, свободах и законных интересах физических лиц, правах и законных интересах юридических лиц и о порядке реализации прав, свобод и законных интересов;

о деятельности государственных органов, общественных объединений;

о правовом статусе государственных органов, за исключением информации, доступ к которой ограничен законодательными актами Республики Беларусь;

о чрезвычайных ситуациях, экологической, санитарно-эпидемиологической обстановке, гидрометеорологической и иной информации, отражающей состояние общественной безопасности;

о состоянии здравоохранения, демографии, образования, культуры, сельского хозяйства;

о состоянии преступности, а также о фактах нарушения законности;

о льготах и компенсациях, предоставляемых государством физическим и юридическим лицам;

о размерах золотого запаса;

об обобщенных показателях по внешней задолженности;

о состоянии здоровья должностных лиц, занимающих должности, включенные в перечень высших государственных должностей Республики Беларусь;

накапливаемой в открытых фондах библиотек и архивов, информационных системах государственных органов, физических и юридических лиц, созданных (предназначенных) для информационного обслуживания физических лиц.

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.

Правовой режим информации, распространение и (или) предоставление которой ограничено, определяется настоящим Законом и иными законодательными актами Республики Беларусь.

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.

Порядок получения, передачи, сбора, обработки, накопления, хранения и предоставления информации о частной жизни физического лица и персональных данных, а также пользования ими устанавливается законодательными актами Республики Беларусь.

Статья 19. Документирование информации

Документирование информации осуществляется ее обладателем в соответствии с требованиями делопроизводства, установленными законодательством Республики Беларусь. Порядок документирования информации, обработки, хранения, распространения и (или) предоставления документированной информации, а также пользования ею устанавливается актами законодательства Республики Беларусь, в том числе техническими нормативными правовыми актами.

ГЛАВА 4 РАСПРОСТРАНЕНИЕ И (ИЛИ) ПРЕДОСТАВЛЕНИЕ ИНФОРМАЦИИ

Статья 20. Распространение и (или) предоставление информации

Распространяемая и (или) предоставляемая информация должна содержать достоверные сведения о ее обладателе, а также о лице, распространяющем и (или) предоставляющем информацию, в форме и объеме, достаточных для идентификации таких лиц.

При использовании для предоставления информации технических средств, позволяющих ознакомить с информацией определенный круг лиц, обладатель информации и информационный посредник обязаны обеспечить пользователям информации возможность свободного отказа от получения предоставляемой таким способом информации.

Если обладателем информации либо информационным посредником или владельцем информационной сети получено уведомление о нежелании конкретного пользователя информации получать распространяемую и (или) предоставляемую информацию, они обязаны принять меры по предотвращению получения такой информации пользователем информации.

При распространении и (или) предоставлении информации по почте, сетям электросвязи лица, распространяющие и (или) предоставляющие информацию, обязаны соблюдать требования законодательства Республики Беларусь о почтовой связи, об электросвязи и о рекламе.

Случаи и требования обязательного распространения и (или) предоставления информации, в том числе предоставления обязательных экземпляров документов, устанавливаются законодательными актами Республики Беларусь и постановлениями Совета Министров Республики Беларусь.

Порядок распространения и (или) предоставления информации, за исключением информации, указанной в части пятой настоящей статьи и части первой статьи 17 настоящего Закона, определяется соглашением субъектов соответствующих информационных отношений, если иное не установлено законодательными актами Республики Беларусь.

Статья 21. Предоставление общедоступной информации по запросу

Предоставление общедоступной информации может осуществляться по запросу заинтересованного государственного органа, физического или юридического лица.

Запросы о получении общедоступной информации могут быть адресованы ее обладателям в форме:

устного запроса;

письменного запроса.

Предоставление заинтересованному государственному органу, физическому или юридическому лицу общедоступной информации по запросу может осуществляться посредством:

устного изложения содержания запрашиваемой информации;

ознакомления с документами, содержащими запрашиваемую информацию;

предоставления копии документа, содержащего запрашиваемую информацию, или выписок из него;

предоставления письменного ответа (справки), содержащего (содержащей) запрашиваемую информацию.

Порядок осуществления устных и письменных запросов о получении общедоступной информации, а также порядок их рассмотрения определяются законодательными актами Республики Беларусь.

Статья 22. Порядок распространения и (или) предоставления общедоступной информации о деятельности государственных органов

Распространение и (или) предоставление общедоступной информации о деятельности государственных органов могут осуществляться посредством ее:

распространения в средствах массовой информации;

размещения в государственном органе в общедоступных местах;

размещения в информационных сетях;

предоставления на основании запросов заинтересованных государственных органов, физических и юридических лиц;

распространения и (или) предоставления иными способами.

Государственные органы обязаны посредством размещения в государственном органе в общедоступных местах распространять, а также могут иными способами распространять и (или) предоставлять следующую информацию:

официальное наименование государственного органа;

адрес места нахождения государственного органа, контактный телефон (факс);

организационную структуру государственного органа (руководство, отделы (управления), контактные телефоны), за исключением информации, доступ к которой ограничен законодательными актами Республики Беларусь;

режим работы государственного органа и время приема физических лиц;

нормативные правовые акты, регламентирующие деятельность государственного органа, за исключением информации, доступ к которой ограничен законодательными актами Республики Беларусь;

официальное наименование, адрес места нахождения и режим работы вышестоящего государственного органа и время приема физических лиц в этом органе.

Кроме информации, указанной в части второй настоящей статьи, в информационных сетях государственные органы обязаны распространять и (или) предоставлять общедоступную информацию о нормативных правовых актах, в том числе технических нормативных правовых актах, принятых данным государственным органом, и иную информацию в соответствии с законодательством Республики Беларусь.

Распространение и (или) предоставление общедоступной информации о деятельности государственных органов осуществляются на безвозмездной основе, если иное не установлено законодательными актами Республики Беларусь.

ГЛАВА 5 ИНФОРМАЦИОННЫЕ РЕСУРСЫ

Статья 23. Виды информационных ресурсов. Правовой режим информационных ресурсов

Информационные ресурсы делятся на государственные и негосударственные.

Состав государственных информационных ресурсов, порядок их формирования, а также пользования документированной информацией из государственных информационных ресурсов определяются Советом Министров Республики Беларусь.

Порядок формирования негосударственных информационных ресурсов определяется собственниками информационных ресурсов.

Статья 24. Государственная регистрация информационных ресурсов

Государственная регистрация информационных ресурсов осуществляется в целях создания единой системы учета и сохранности информационных ресурсов, создания условий для их передачи на государственное архивное хранение, информирования государственных органов, физических и юридических лиц о составе и содержании информационных ресурсов в Республике Беларусь.

Государственная регистрация информационных ресурсов осуществляется Министерством связи и информатизации Республики Беларусь путем внесения сведений об информационных ресурсах в Государственный регистр информационных ресурсов.

Порядок государственной регистрации информационных ресурсов, за исключением информационных ресурсов, указанных в части четвертой настоящей статьи, и порядок ведения Государственного регистра информационных ресурсов определяются Советом Министров Республики Беларусь.

Порядок регистрации информационных ресурсов, формируемых органами государственной безопасности Республики Беларусь, определяется Комитетом государственной безопасности Республики Беларусь.

Государственной регистрации подлежат государственные информационные ресурсы.

Негосударственные информационные ресурсы регистрируются в Государственном регистре информационных ресурсов на добровольной основе.

ГЛАВА 6 ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ИНФОРМАЦИОННЫЕ СЕТИ

Статья 25. Создание и использование информационных технологий, информационных систем и информационных сетей

Создание информационных технологий, информационных систем и информационных сетей осуществляется государственными органами, физическими и юридическими лицами.

Информационные системы делятся на государственные и негосударственные.

Государственные информационные системы создаются в целях предоставления общедоступной информации, обеспечения ее объективности, полноты и достоверности,

оказания информационных услуг, оптимизации деятельности государственных органов и обеспечения информационного обмена между ними.

Государственные информационные системы создаются в порядке и на условиях, определенных законодательством Республики Беларусь.

Порядок использования государственных информационных систем определяется Советом Министров Республики Беларусь.

Негосударственные информационные системы создаются физическими и юридическими лицами в целях удовлетворения своих информационных потребностей и (или) оказания информационных услуг.

Порядок создания и использования негосударственных информационных систем определяется их собственниками или уполномоченными ими лицами.

Порядок включения информационных систем в информационные сети, а также правила обмена информацией в них устанавливаются их собственниками или уполномоченными ими лицами.

Порядок использования информационных систем и информационных сетей в случае, когда собственниками программно-технических средств и информационных систем являются разные лица, определяется соглашением между этими лицами.

Идентификация лиц, участвующих в информационном обмене с использованием информационных систем и информационных сетей, осуществляется в случаях, установленных актами законодательства Республики Беларусь.

Статья 26. Государственная регистрация информационных систем

Государственная регистрация информационных систем осуществляется в целях создания единой системы учета информационных систем, обеспечения их сохранности, а также информирования государственных органов, физических и юридических лиц об информационных системах в Республике Беларусь.

Государственная регистрация информационных систем, за исключением информационных систем, указанных в части четвертой настоящей статьи, осуществляется Министерством связи и информатизации Республики Беларусь путем внесения сведений об информационных системах в Государственный регистр информационных систем.

Порядок государственной регистрации информационных систем, за исключением информационных систем, указанных в части четвертой настоящей статьи, и порядок ведения Государственного регистра информационных систем определяются Советом Министров Республики Беларусь.

Порядок государственной регистрации информационных систем, содержащих государственные секреты, определяется Комитетом государственной безопасности Республики Беларусь.

Государственной регистрации подлежат государственные информационные системы.

Негосударственные информационные системы регистрируются в Государственном регистре информационных систем на добровольной основе.

ГЛАВА 7 ЗАЩИТА ИНФОРМАЦИИ

Статья 27. Цели защиты информации

Целями защиты информации являются:

обеспечение национальной безопасности, суверенитета Республики Беларусь;

сохранение информации о частной жизни физических лиц и неразглашение персональных данных, содержащихся в информационных системах;

обеспечение прав субъектов информационных отношений при создании, использовании и эксплуатации информационных систем и информационных сетей,

использовании информационных технологий, а также формировании и использовании информационных ресурсов;

недопущение неправомерного доступа, уничтожения, модификации (изменения), копирования, распространения и (или) предоставления информации, блокирования правомерного доступа к информации, а также иных неправомерных действий.

Статья 28. Основные требования по защите информации

Защите подлежит информация, неправомерные действия в отношении которой могут причинить вред ее обладателю, пользователю или иному лицу.

Требования по защите общедоступной информации могут устанавливаться только в целях недопущения ее уничтожения, модификации (изменения), блокирования правомерного доступа к ней.

Требования по защите информации в государственных информационных системах, а также информационных системах, содержащих информацию, распространение и (или) предоставление которой ограничено, определяются законодательством Республики Беларусь.

Информация, распространение и (или) предоставление которой ограничено, а также информация, содержащаяся в государственных информационных системах, должны обрабатываться в информационных системах с применением системы защиты информации, аттестованной в порядке, установленном Советом Министров Республики Беларусь.

Не допускается эксплуатация государственных информационных систем без реализации мер по защите информации.

Обеспечение целостности и сохранности информации, содержащейся в государственных информационных системах, осуществляется путем установления и соблюдения единых требований по защите информации от неправомерного доступа, уничтожения, модификации (изменения) и блокирования правомерного доступа к ней, в том числе при осуществлении доступа к информационным сетям.

Для создания системы защиты информации используются средства защиты информации, имеющие сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам государственной экспертизы, порядок проведения которой определяется Советом Министров Республики Беларусь.

Физические и юридические лица, занимающиеся созданием средств защиты информации и реализацией мер по защите информации, осуществляют свою деятельность в этой области на основании специальных разрешений (лицензий), выдаваемых государственными органами, уполномоченными Президентом Республики Беларусь, в соответствии с законодательством Республики Беларусь о лицензировании.

Статья 29. Меры по защите информации

К правовым мерам по защите информации относятся заключаемые обладателем информации с пользователем информации договоры, в которых устанавливаются условия пользования информацией, а также ответственность сторон по договору за нарушение указанных условий.

К организационным мерам по защите информации относятся обеспечение особого режима допуска на территории (в помещения), где может быть осуществлен доступ к информации (материальным носителям информации), а также разграничение доступа к информации по кругу лиц и характеру информации.

К техническим (программно-техническим) мерам по защите информации относятся меры по использованию средств защиты информации, в том числе криптографических, а также систем контроля доступа и регистрации фактов доступа к информации.

Государственные органы и юридические лица, осуществляющие обработку информации, распространение и (или) предоставление которой ограничено, определяют соответствующие структурные подразделения или должностных лиц, ответственных за обеспечение защиты информации.

Статья 30. Организация защиты информации

Защита информации организуется:

в отношении общедоступной информации – лицом, осуществляющим распространение и (или) предоставление такой информации;

в отношении информации, распространение и (или) предоставление которой ограничено, – собственником или оператором информационной системы, содержащей такую информацию, либо обладателем информации, если такая информация не содержится в информационных системах;

иными лицами в случаях, определенных настоящим Законом и иными законодательными актами Республики Беларусь.

Статья 31. Права и обязанности субъектов информационных отношений по защите информации

Обладатель информации, собственник программно-технических средств, информационных ресурсов, информационных систем и информационных сетей или уполномоченные ими лица вправе:

запрещать или приостанавливать обработку информации и (или) пользование ею в случае невыполнения требований по защите информации;

обращаться в государственные органы, определенные Президентом Республики Беларусь и (или) Советом Министров Республики Беларусь, для оценки правильности выполнения требований по защите их информации в информационных системах, проведения экспертизы достаточности мер по защите их программно-технических средств, информационных ресурсов, информационных систем и информационных сетей, а также для получения консультаций.

Владелец информационных систем и информационных сетей обязан уведомить их собственника, а также обладателя информации о всех фактах нарушения требований по защите информации.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Республики Беларусь, обязаны:

обеспечить защиту информации, а также постоянный контроль за соблюдением требований по защите информации;

установить порядок предоставления информации пользователю информации и определить необходимые меры по обеспечению условий доступа к информации пользователя информации;

не допускать воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

обеспечивать возможность незамедлительного восстановления информации, модифицированной (измененной) или уничтоженной вследствие неправомерного (несанкционированного) доступа к ней.

Статья 32. Защита персональных данных

Меры по защите персональных данных от разглашения должны быть приняты с момента, когда персональные данные были предоставлены физическим лицом, к которому они относятся, другому лицу либо когда предоставление персональных данных осуществляется в соответствии с законодательными актами Республики Беларусь.

Последующая передача персональных данных разрешается только с согласия физического лица, к которому они относятся, либо в соответствии с законодательными актами Республики Беларусь.

Меры, указанные в части первой настоящей статьи, должны приниматься до уничтожения персональных данных, либо до их обезличивания, либо до получения согласия физического лица, к которому эти данные относятся, на их разглашение.

Субъекты информационных отношений, получившие персональные данные в нарушение требований настоящего Закона и иных законодательных актов Республики Беларусь, не вправе пользоваться ими.

ГЛАВА 8. ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТОВ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЕ ИНФОРМАЦИИ

Статья 33. Права и обязанности обладателя информации

Обладатель информации в отношении информации, которой он обладает, имеет право:

распространять и (или) предоставлять информацию, пользоваться ею;

разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа в соответствии с законодательными актами Республики Беларусь;

требовать указания себя в качестве источника информации, ставшей общедоступной по его решению, при ее распространении и (или) предоставлении другими лицами;

определять условия обработки информации и пользования ею в информационных системах и информационных сетях;

передавать права на пользование информацией в соответствии с законодательством Республики Беларусь или по договору;

защищать в установленном законодательством Республики Беларусь порядке свои права в случае незаконного получения информации или незаконного пользования ею иными лицами;

осуществлять меры по защите информации;

осуществлять иные действия в соответствии с настоящим Законом и иными актами законодательства Республики Беларусь.

Права обладателя информации, содержащейся в информационном ресурсе, подлежат охране независимо от авторских и иных прав на информационный ресурс.

Права обладателя информации не распространяются на программно-технические средства, информационные системы и информационные сети, принадлежащие собственнику, с помощью которых осуществляются поиск, получение, передача, сбор, обработка, накопление, хранение, распространение и (или) предоставление информации, пользование информацией.

Обладатель информации обязан:

соблюдать права и законные интересы иных лиц при распространении и (или) предоставлении информации, которой он обладает, а также при пользовании ею;

принимать меры по защите информации, если такая обязанность установлена законодательными актами Республики Беларусь;

распространять и (или) предоставлять информацию, в отношении которой законодательными актами Республики Беларусь установлена обязательность ее распространения и (или) предоставления;

предоставлять достоверную, полную информацию в установленный срок;

ограничивать и (или) запрещать доступ к информации, если такая обязанность установлена законодательными актами Республики Беларусь;

обеспечивать сохранность информации, распространение и (или) предоставление которой ограничено;

исполнять другие обязанности в соответствии с настоящим Законом и иными законодательными актами Республики Беларусь.

Статья 34. Права и обязанности пользователя информации

Пользователь информации имеет право:

получать, распространять и (или) предоставлять информацию;

использовать информационные технологии, информационные системы и информационные сети;

знакомиться со своими персональными данными;

осуществлять иные действия в соответствии с настоящим Законом и иными актами законодательства Республики Беларусь.

Пользователь информации обязан:

соблюдать права и законные интересы других лиц при использовании информационных технологий, информационных систем и информационных сетей;

принимать меры по защите информации, если такая обязанность установлена законодательными актами Республики Беларусь;

обеспечивать сохранность информации, распространение и (или) предоставление которой ограничено, и не передавать ее полностью или частично третьим лицам без согласия обладателя информации;

исполнять другие обязанности в соответствии с настоящим Законом и иными законодательными актами Республики Беларусь.

Статья 35. Права и обязанности пользователя информационной системы и (или) информационной сети

Пользователь информационной системы и (или) информационной сети имеет право:

использовать информационную систему и (или) информационную сеть для доступа к информационным ресурсам;

получать, распространять и (или) предоставлять информацию, содержащуюся в информационной системе и (или) информационной сети;

осуществлять иные действия в соответствии с настоящим Законом и иными актами законодательства Республики Беларусь.

Пользователь информационной системы и (или) информационной сети обязан:

соблюдать права других лиц при использовании информационной системы и (или) информационной сети;

исполнять другие обязанности в соответствии с настоящим Законом и иными законодательными актами Республики Беларусь.

Статья 36. Права и обязанности собственника информационных ресурсов

Собственник информационных ресурсов, если иное не предусмотрено настоящим Законом и иными законодательными актами Республики Беларусь, имеет право:

предоставлять права владения и пользования информационными ресурсами иному лицу;

определять правила обработки информации, использования информационных ресурсов;

определять условия распоряжения документированной информацией в случае ее распространения и (или) предоставления по договору;

осуществлять иные действия в соответствии с настоящим Законом и иными актами законодательства Республики Беларусь.

Собственник информационных ресурсов обязан:

определять условия владения и пользования информационными ресурсами в случае, предусмотренном абзацем вторым части первой настоящей статьи;

осуществлять меры по защите информационных ресурсов, если такая обязанность установлена законодательными актами Республики Беларусь;

исполнять другие обязанности в соответствии с настоящим Законом и иными законодательными актами Республики Беларусь.

Статья 37. Права и обязанности собственника программно-технических средств, информационных систем и информационных сетей

Собственником программно-технических средств, используемых для создания информационной системы, и собственником информационной системы, образующих информационную сеть, могут являться как одно, так и несколько лиц.

Собственник программно-технических средств, информационных систем и информационных сетей вправе передать иному лицу права владения и пользования программно-техническими средствами, информационными системами и информационными сетями.

Права на информацию, включенную в состав информационных систем, определяются соглашением между обладателями информации и собственниками информационных систем.

Правомочия собственника государственной информационной системы осуществляет заказчик по государственному контракту на выполнение подрядных работ для государственных нужд по созданию такой информационной системы, если иное не указано в решении о ее создании.

Собственник информационной системы вправе, если иное не установлено обладателем информации, запретить или ограничить передачу, распространение и (или) предоставление информации.

Собственник программно-технических средств, информационных систем и информационных сетей обладает другими правами в соответствии с настоящим Законом и иными актами законодательства Республики Беларусь, исполняет обязанности в соответствии с настоящим Законом и иными законодательными актами Республики Беларусь.

Статья 38. Права и обязанности владельца программно-технических средств, информационных ресурсов, информационных систем и информационных сетей

Владелец программно-технических средств, информационных ресурсов, информационных систем и информационных сетей имеет право:

определять условия их использования с соблюдением исключительных прав на объекты интеллектуальной собственности;

осуществлять иные действия в соответствии с настоящим Законом и иными актами законодательства Республики Беларусь.

Владелец программно-технических средств, информационных ресурсов, информационных систем и информационных сетей обязан:

осуществлять меры по защите информации;

исполнять другие обязанности в соответствии с настоящим Законом и иными законодательными актами Республики Беларусь.

Статья 39. Права и обязанности информационного посредника

Информационный посредник обладает правами в соответствии с настоящим Законом и иными актами законодательства Республики Беларусь.

Информационный посредник обязан обеспечить предоставление информационных услуг обладателю и (или) пользователю информации по их запросам или в соответствии с условиями договора между информационным посредником и обладателем или пользователем информации либо уполномоченными ими лицами.

Информационному посреднику запрещается распространять и (или) предоставлять третьим лицам информацию, полученную при предоставлении информационных услуг, кроме случаев, предусмотренных законодательством Республики Беларусь.

Информационный посредник исполняет другие обязанности в соответствии с настоящим Законом и иными законодательными актами Республики Беларусь.

Статья 40. Права и обязанности оператора информационной системы

Оператор информационной системы имеет право:

осуществлять эксплуатацию информационной системы в порядке и на условиях, определенных договором, заключенным с ее владельцем;

определять порядок эксплуатации информационной системы в случае, если он является ее владельцем;

осуществлять иные действия в соответствии с настоящим Законом и иными актами законодательства Республики Беларусь.

Оператор информационной системы обязан:

обеспечить целостность и сохранность информации, содержащейся в информационной системе;

принимать меры по предотвращению разглашения, утраты, искажения, уничтожения, модификации (изменения) информации и блокирования правомерного доступа к ней, а при необходимости – меры по восстановлению утраченной информации;

исполнять другие обязанности в соответствии с настоящим Законом и иными законодательными актами Республики Беларусь.

Статья 41. Ответственность за нарушение законодательства об информации, информатизации и защите информации

Нарушение законодательства об информации, информатизации и защите информации влечет ответственность в соответствии с законодательными актами Республики Беларусь.

2. СОДЕРЖАНИЕ ОТЧЕТА

Цель работы.

Решение задания. Аналитический обзор законов по правовому обеспечению информационной безопасности.

Ответы на контрольные вопросы.

3. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Определите сферу действия Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации».

2. На чём основывается законодательство об информации, информатизации и защите информации?

3. На каких принципах базируется правовое регулирование информационных отношений?

4. Перечислите субъектов информационных отношений.

5. В каких случаях право на информацию не может быть использовано?

6. Что включает государственное регулирование в области информации, информатизации и защиты информации?

7. Кем осуществляется государственное регулирование и управление в области информации, информатизации и защиты информации?

8. Какая информация относится к общедоступной и ограниченной?

9. Как определена законодательством информация о частной жизни физического лица и персональные данные?

10. В каких целях осуществляется государственная регистрация информационных ресурсов?

11. Перечислите основные требования по защите информации?

12. Назовите основные меры по защите информации.

13. Как законодательно осуществляется защита персональных данных?

14. Перечислите права и обязанности пользователя информационной системы и (или) информационной сети?

15. Что понимается под грифом секретности?

16. Что или кто является носителем государственных секретов?

17. Кем осуществляется государственное регулирование и управление в сфере государственных секретов?

18. Какие сведения могут быть отнесены к государственным секретам?

19. Права и обязанности граждан по отношению к госсекретам?

20. Какими полномочиями обладают государственные органы и иные организации, наделенные полномочиями по отнесению сведений к государственным секретам?

21. Перечислите категории, степени и грифы секретности.

22. Кому принадлежит право собственности на государственные секреты?

23. Как организуется защита государственных секретов?

24. В чём состоят условия предоставления гражданам допуска к государственным секретам?

СПИСОК ИСТОЧНИКОВ

Основная литература:

1. [Электрон, ресурс] – http://www.minfin.gov.by/upload/gosznak/acts/zakon_190710_170z.pdf
Закон Республики Беларусь 19 июля 2010 г. №170-З «О Государственных Секретах»

2. [Электрон, ресурс] – http://www.pravo.by/main.aspx?guid=3871&p0=h10800455&p2={NRPA}
Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации»

ПРАКТИЧЕСКАЯ РАБОТА №3

ТЕМА: Международные стандарты информационной безопасности

ЦЕЛЬ РАБОТЫ: Изучить международные стандарты, определяющие требования к системам управления информационной безопасностью, управление рисками, метрики и измерения, а также руководство по внедрению.

Результат обучения:

После успешного завершения занятия пользователь должен:

- знать международные стандарты, определяющие требования к системам управления информационной безопасностью, управление рисками, метрики и измерения, а также руководство по их внедрению.

Используемая программа: Firefox, Internet Explorer, Opera и др.

План занятия:

1. Изучение кратких теоретических сведений.
2. Выполнение задания.
3. Оформление отчета.

1. КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

В соответствии с международными и национальными стандартами обеспечение информационной безопасности в любой компании предполагает следующее:

- определение целей обеспечения информационной безопасности компьютерных систем;
- создание эффективной системы управления информационной безопасностью;
- расчет совокупности детализированных качественных и количественных показателей для оценки соответствия информационной безопасности поставленным целям;
- применение инструментария обеспечения информационной безопасности и оценки ее текущего состояния;
- использование методик управления безопасностью, позволяющих объективно оценить защищенность информационных активов и управлять информационной безопасностью компании.

Рассмотрим наиболее известные международные стандарты в области защиты информации, которые могут быть использованы в отечественных условиях.

Стандарты ISO/IEC 17799:2002 (BS 7799:2000)

Международный стандарт ISO/IEC 17799:2000 (BS 7799-1:2000) «Управление информационной безопасностью – Информационные технологии» («Information technology – Information security management*) является одним из наиболее известных стандартов в области защиты информации.

Данный стандарт был разработан на основе первой части Британского стандарта BS 7799—1:1995 «Практические рекомендации по управлению информационной безопасностью» («Information security management – Part 1:Code of practice forinformation security management*) и относится к новому поколению стандартов информационной безопасности компьютерных ИС.

Текущая версия стандарта ISO/IEC 17799:2000 (BS 7799—1:2000) рассматривает следующие актуальные вопросы обеспечения информационной безопасности организаций и предприятий:

- необходимость обеспечения информационной безопасности;
- основные понятия и определения информационной безопасности;
- политика информационной безопасности компании;
- организация информационной безопасности на предприятии;
- классификация и управление корпоративными информационными ресурсами;
- кадровый менеджмент и информационная безопасность;
- физическая безопасность;
- администрирование безопасности КИС;
- управление доступом;
- требования по безопасности к КИС в ходе их разработки, эксплуатации и сопровождения;
- управление бизнес-процессами компании с точки зрения информационной безопасности;
- внутренний аудит информационной безопасности компании.

Вторая часть стандарта BS 7799—2:2000 «Спецификации систем управления информационной безопасностью» («Information security management – Part 2:Specification forinformation security management systems»), определяет возможные функциональные спецификации корпоративных систем управления информационной безопасностью с точки зрения их проверки на соответствие требованиям первой части данного стандарта. В соответствии с положениями этого стандарта также регламентируется процедура аудита КИС.

Дополнительные рекомендации для управления информационной безопасностью содержат руководства Британского института стандартов – British Standards Institution (BSI), изданные в 1995—2003 гг. в виде следующей серии:

- «Введение в проблему управления информационной безопасностью» («Information security managment: an introduction*);
- «Возможности сертификации на требования стандарта BS 7799» («Preparingfor BS 7799 sertification»);
- «Руководство BS 7799 по оценке и управлению рисками» («Guideto BS 7799 risk assessment and risk management*);
- «Руководство для проведения аудита на требования стандарта» («BS 7799 Guideto BS 7799 auditing*);
- «Практические рекомендации по управлению безопасностью информационных технологий» («Code of practice for IT management*).

В 2002 г. международный стандарт ISO 17799 (BS 7799) был пересмотрен и существенно дополнен. В новом варианте этого стандарта большое внимание уделено вопросам повышения культуры защиты информации в различных международных компаниях. По мнению специалистов, обновление международного стандарта ISO 17799 (BS 7799) позволит не только повысить культуру защиты информационных активов компании, но и скоординировать действия различных ведущих государственных и коммерческих структур в области защиты информации.

Германский стандарт BSI

В отличие от ISO 17799 германское «Руководство по защите информационных технологий для базового уровня защищенности» посвящено детальному рассмотрению частных вопросов управления информационной безопасностью компании.

В германском стандарте BSI представлены:

- общая методика управления информационной безопасностью (организация менеджмента в области информационной безопасности, методология использования руководства);
- описания компонентов современных ИТ;
- описания основных компонентов организации режима информационной безопасности (организационный и технический уровни защиты данных, планирование действий в чрезвычайных ситуациях, поддержка непрерывности бизнеса);
- характеристики объектов информатизации (здания, помещения, кабельные сети, контролируемые зоны);
- характеристики основных информационных активов компании (в том числе аппаратное и программное обеспечение, например рабочие станции и серверы под управлением ОС семейства DOS, Windows и UNIX);
- характеристики компьютерных сетей на основе различных сетевых технологий, например сети Novell Net Ware, сети UNIX и Windows);
- характеристика активного и пассивного телекоммуникационного оборудования ведущих поставщиков, например Cisco Systems;
- подробные каталоги угроз безопасности и мер контроля (более 600 наименований в каждом каталоге).

Вопросы защиты приведенных информационных активов компании рассматриваются по определенному сценарию: общее описание информационного актива компании – возможные угрозы и уязвимости безопасности – возможные меры, и средства контроля и защиты.

Международный стандарт ISO 15408 «Общие критерии безопасности информационных технологий»

Одним из главных результатов стандартизации в сфере систематизации требований и характеристик защищенных информационных комплексов стала система международных и национальных стандартов безопасности информации, которая насчитывает более сотни различных документов. Важное место в этой системе стандартов занимает стандарт ISO 15408, известный как «Common Criteria, CC»*.

В 1990 г. Международная организация по стандартизации (ISO) приступила к разработке международного стандарта по критериям оценки безопасности ИТ для общего использования. В разработке участвовали:

- Национальный институт стандартов и технологии и Агентство национальной безопасности (США),
- Учреждение безопасности коммуникаций (Канада),
- Агентство информационной безопасности (Германия),
- Агентство национальной безопасности коммуникаций (Голландия),
- органы исполнения Программы безопасности и сертификации ИТ (Англия),
- Центр обеспечения безопасности систем (Франция),

которые опирались на свой солидный задел.

За десятилетие разработки лучшими специалистами мира документ неоднократно редактировался. Первые две версии были опубликованы соответственно в январе и мае 1998 г. Версия 2.1 этого стандарта утверждена 8 июня 1999 г. Международной организацией по стандартизации (ISO) в качестве международного стандарта информационной безопасности ISO/IEC 15408 под названием «Общие критерии оценки безопасности информационных технологий», или «Common Criteria for Information Technology Security Evaluation»*.

«Общие критерии» (ОК) обобщили содержание и опыт использования Оранжевой книги, развили европейские и канадские критерии и воплотили в реальные структуры концепцию типовых профилей защиты федеральных критериев США.

В ОК проведена классификация широкого набора требований безопасности ИТ, определены структуры их группирования и принципы использования. Главные достоинства ОК – полнота требований безопасности и их систематизация, гибкость в применении и открытость для последующего развития.

Ведущие мировые производители оборудования ИТ сразу стали поставлять заказчикам средства, полностью отвечающие требованиям ОК.

ОК разрабатывались для удовлетворения запросов трех групп специалистов, в равной степени являющихся пользователями этого документа: производителей и потребителей продуктов ИТ, а также экспертов по оценке уровня их безопасности. ОК обеспечивают нормативную поддержку процесса выбора ИТ-продукта, к которому предъявляются требования функционирования в условиях действия определенных угроз, служат руководящим материалом для разработчиков таких систем, а также регламентируют технологию их создания и процедуру оценки обеспечиваемого уровня безопасности.

ОК рассматривают информационную безопасность, во-первых, как совокупность конфиденциальности и целостности информации, обрабатываемой ИТ-продуктом, а также доступности ресурсов ВС и, во-вторых, ставят перед средствами защиты задачу противодействия угрозам, актуальным для среды эксплуатации этого продукта и реализации политики безопасности, принятой в этой среде эксплуатации. Поэтому в концепцию ОК входят все аспекты процесса проектирования, производства и эксплуатации ИТ-продуктов, предназначенных для работы в условиях действия определенных угроз безопасности.

Потребители ИТ-продуктов озабочены наличием угроз безопасности, приводящих к определенным рискам для обрабатываемой информации. Для противодействия этим угрозам ИТ-продукты должны включать в свой состав средства защиты, противодействующие этим угрозам и направленные на устранение уязвимостей, однако ошибки в средствах защиты в свою очередь могут приводить к появлению новых уязвимостей. Сертификация средств защиты позволяет подтвердить их адекватность угрозам и рискам.

ОК регламентируют все стадии разработки, квалификационного анализа и эксплуатации ИТ-продуктов. ОК предлагают концепцию процесса разработки и квалификационного анализа ИТ-продуктов, требующую от потребителей и производителей большой работы по составлению и оформлению объемных и подробных нормативных документов.

Требования ОК являются практически всеобъемлющей энциклопедией информационной безопасности, поэтому их можно использовать в качестве справочника по безопасности ИТ.

Стандарт ISO 15408 поднял стандартизацию ИТ на межгосударственный уровень. Возникла реальная перспектива создания единого безопасного информационного пространства, в котором сертификация безопасности систем обработки информации будет осуществляться на глобальном уровне, что предоставит возможности для интеграции национальных ИС, что в свою очередь откроет новые сферы применения ИТ.

Принятый базовый стандарт информационной безопасности ISO 15408, безусловно, очень важен и для белорусов.

Стандарты для беспроводных сетей

Стандарт IEEE 802.11

В 1990 г. Комитет IEEE 802 сформировал рабочую группу 802.11 для разработки стандарта для беспроводных локальных сетей. Работы по созданию стандарта были завершены через 7 лет. В 1997 г. была ратифицирована первая спецификация беспроводного стандарта IEEE 802.11, обеспечивающего передачу данных с гарантированной скоростью 1 Мб/с (в некоторых случаях до 2 Мб/с) в полосе частот 2,4 ГГц. Эта полоса частот доступна для нелицензионного использования в большинстве стран мира.

Стандарт IEEE 802.11 является базовым стандартом и определяет протоколы, необходимые для организации беспроводных локальных сетей WLAN (Wireless Local Area Network). Основные из них – протокол управления доступом к среде MAC (Medium Accsess Control – нижний подуровень канального уровня) и протокол PHY передачи сигналов в физической среде. В качестве физической среды допускается использование радиоволн и инфракрасного излучения.

В основу стандарта IEEE 802.11 положена сотовая архитектура, причем сеть может состоять как из одной, так и нескольких ячеек. Каждая из них управляется базовой станцией, называемой точкой доступа AP (Access Point), которая вместе с находящимися в пределах радиуса ее действия рабочими станциями пользователей образует базовую зону обслуживания BSS (Basic Service Set). Точки доступа многосотовой сети взаимодействуют между собой через распределительную систему DS (Distribution System), представляющую собой эквивалент магистрального сегмента кабельных ЛС. Вся инфраструктура, включающая точки доступа и распределительную систему образует расширенную зону обслуживания ESS (Extended Service Set). Стандартом предусмотрен также односотовый вариант беспроводной сети, который может быть реализован и без точки доступа, при этом часть ее функций выполняются непосредственно рабочими станциями.

Для обеспечения перехода мобильных рабочих станций из зоны действия одной точки доступа к другой в многосотовых системах предусмотрены специальные процедуры сканирования (активного и пассивного прослушивания эфира) и присоединения (Association), однако строгих спецификаций по реализации роуминга стандарт IEEE 802.11 не предусматривает.

Для защиты WLAN стандартом IEEE 802.11 предусмотрен алгоритм WEP (Wired Equivalent Privacy). Он включает средства противодействия НСД к сети, а также шифрование для предотвращения перехвата информации.

Однако заложенная в первую спецификацию стандарта IEEE 802.1 1 скорость передачи данных в беспроводной сети перестала удовлетворять потребностям пользователей: алгоритм WEP имел ряд существенных недостатков – отсутствие управления ключом, использование общего статического ключа, малые разрядности ключа и вектора инициализации, сложности использования алгоритма RC4.

Чтобы сделать технологию Wireless LAN недорогой, популярной и удовлетворяющей жестким требованиям бизнес-приложений, разработчики создали семейство новых спецификаций стандарта IEEE 802.11 – a, b, L Стандарты этого семейства, по сути, являются беспроводными расширениями протокола Ethernet, что обеспечивает хорошее взаимодействие с проводными сетями Ethernet.

Стандарт IEEE 802.11 b

Стандарт IEEE 802.11 b был ратифицирован IEEE в сентябре 1999 г. как развитие базового стандарта 802.11; в нем используется полоса частот 2,4 ГГц, скорость передачи достигает 11 Мб/с (подобно Ethernet). Благодаря ориентации на освоенный диапазон 2,4 ГГц стандарт 802.11 b завоевал большую популярность у производителей оборудования. В качестве базовой радиотехнологии в нем используется метод распределенного спектра с прямой последовательностью DSSS (Direct Sequence Spread Spectrum), который отличается высокой устойчивостью к искажению данных помехами, в том числе преднамеренными. Этот

стандарт получил широкое распространение, и беспроводные LAN стали привлекательным решением с технической и финансовой точки зрения.

Стандарт IEEE 802.11 a

Стандарт IEEE 802.11 a предназначен для работы в частотном диапазоне 5 ГГц. Скорость передачи данных до 54 Мбит/с, т. е. примерно в 5 раз быстрее сетей 802.1 lb. Ассоциация WECA называет этот стандарт Wi-Fi5. Это наиболее широкополосный стандарт из семейства стандартов 802.11. Определены три обязательные скорости – 6, 12 и 24 Мбит/с и пять необязательных – 9, 18, 36, 48 и 54 Мбит/с. В качестве метода модуляции сигнала принято ортогональное частотное мультиплексирование OFDM (Orthogonal Frequency Division Multiplexing). Его отличие от метода DSSS заключается в том, что OFDM предполагает параллельную передачу полезного сигнала одновременно по нескольким частотам диапазона, в то время как технологии расширения спектра DSSS передают сигналы последовательно. В результате повышается пропускная способность канала и качество сигнала. К недостаткам стандарта 802.11 относится большая потребляемая мощность радиопередатчиков для частот 5 ГГц, а также меньший радиус действия (около 100 м).

Для простоты запоминания в качестве общего имени для стандартов 802.1 lb и 802.11 a, а также всех последующих, относящихся к беспроводным локальным сетям (WLAN), Ассоциацией беспроводной совместимости с Ethernet WECA (Wireless Ethernet Compatibility Aliance) был введен термин Wi-Fi (Wireless Fidelity). Если устройство помечено этим знаком, оно протестировано на совместимость с другими устройствами 802.11.

Стандарт IEEE 802.1 lg

Стандарт IEEE 802.1 lg представляет собой развитие 802.11 b и обратно совместим с 802.11 b; предназначен для обеспечения скоростей передачи данных до 54 Мбит/с. В числе достоинств 802.1 lg надо отметить низкую потребляемую мощность, большие расстояния (до 300 м) и высокую проникающую способность сигнала.

Стандарт IEEE 802.1 li

Стандарт IEEE 802.1 li – стандарт обеспечения безопасности в беспроводных сетях; ратифицирован IEEE в 2004 г. Этот стандарт решил существовавшие проблемы в области аутентификации и протокола шифрования, обеспечив значительно более высокий уровень безопасности. Стандарт 802.1 li может применяться в сетях Wi-Fi, независимо от используемого стандарта – 802.1 la, b или g.

Стандарты WPA и 802.1 n.

Существуют два очень похожих стандарта – WPA и 802.1 n. WPA был разработан в Wi-Fi Alliance как решение, которое можно применить немедленно, не дожидаясь завершения длительной процедуры ратификации 802.1 li в IEEE. Оба стандарта используют механизм 802.1 x (см. далее) для обеспечения надежной аутентификации, оба используют сильные алгоритмы шифрования и предназначены для замены протокола WEP.

Их основное отличие заключается в использовании различных механизмов шифрования. В WPA применяется протокол TKIP (Temporal Key Integrity Protocol), который, также как и WEP, использует шифр RC4, но значительно более безопасным способом. Обеспечение конфиденциальности данных в стандарте IEEE 802.1 li основано на использовании алгоритма шифрования AES (Advanced Encryption Standard). Использующий его защитный протокол получил название CCMP (Counter-Mode CBC MAC Protocol). Алгоритм AES обладает высокой криптостойкостью. Длина ключа AES равна 128, 192 или 256 бит, что обеспечивает наиболее надежное шифрование из доступных сейчас.

Стандарт 802.1 П предполагает наличие трех участников процесса аутентификации. Это сервер аутентификации AS (Authentication Server), точка доступа AP (Access Point) и рабочая станция STA (Station). В процессе шифрования данных участвуют только AP и STA (AS не используется). Стандарт предусматривает двустороннюю аутентификацию (в отличие от WEP, где аутентифицируется только рабочая станция, но не точка доступа). При этом

местами принятия решения о разрешении доступа являются сервер аутентификации AS и рабочая станция STA, а местами исполнения этого решения – точка доступа AP и STA.

Для работы по стандарту 802.1 li создается иерархия ключей, содержащая мастер-ключ MK (Master Key), парный мастер-ключ PMK (Pairwise Master Key), парный временный ключ PTK (Pairwise Transient Key), а также групповые временные ключи GTK (Group Transient Key), служащие для защиты широковещательного сетевого трафика.

MK – это симметричный ключ, реализующий решение STA и AS о взаимной аутентификации. Для каждой сессии создается новый MK.

PMK – обновляемый симметричный ключ, владение которым означает разрешение (авторизацию) на доступ к среде передачи данных в течение данной сессии. PMK создается на основе MK. Для каждой пары STA и AP в каждой сессии создается новый PMK.

PTK – это коллекция операционных ключей, которые используются для привязки PMK к данным STA и AP, распространения GTK и шифрования данных.

Процесс аутентификации и доставки ключей определяется стандартом 802.1 x. Он предоставляет возможность использовать в беспроводных сетях такие традиционные серверы аутентификации, как RADIUS (Remote Authentication Dial-InUser Server). Стандарт 802.1 li не определяет тип сервера аутентификации, но использование RADIUS для этой цели является стандартным решением.

Транспортом для сообщений 802.1 x служит протокол EAP (Extensible Authentication Protocol). EAP позволяет легко добавлять новые методы аутентификации. Точке доступа не требуется знать об используемом методе аутентификации, поэтому изменение метода никак не затрагивает точку доступа. Наиболее популярные методы EAP – это LEAP, PEAP, TTLS и FAST. Каждый из методов имеет свои сильные и слабые стороны, условия применения, по-разному поддерживается производителями оборудования и ПО. Выделяют пять фаз работы 802.1 n.

Первая фаза – обнаружение. В этой фазе рабочая станция STA находит точку доступа AP, с которой может установить связь и получает от нее используемые в данной сети параметры безопасности. Таким образом STA узнает идентификатор сети SSID и методы аутентификации, доступные в данной сети. Затем STA выбирает метод аутентификации, и между STA и AP устанавливается соединение. После этого STA и AP готовы к началу второй фазы 802.1 x.

Вторая фаза – аутентификация. В этой фазе выполняется взаимная аутентификация STA и сервера AS, создаются MK и PMK. В данной фазе STA и AP блокируют весь трафик, кроме трафика 802.1 x.

Третья фаза – AS перемещает ключ PMK на AP. Теперь STA и AP владеют действительными ключами PMK.

Четвертая фаза – управление ключами 802.1 x. В этой фазе происходит генерация, привязка и верификация ключа PTK.

Пятая фаза – шифрование и передача данных. Для шифрования используется соответствующая часть PTK.

Стандартом 802.1 li предусмотрен режим PSK (Pre-SharedKey), который позволяет обойтись без сервера аутентификации AS. При использовании этого режима на STA и на AP вручную вводится Pre-SharedKey, который используется в качестве PMK. Дальше генерация PTK происходит описанным выше порядком. Режим PSK может использоваться в небольших сетях, где нецелесообразно устанавливать AS.

Стандарты информационной безопасности в Интернете

По оценке Комитета ООН по предупреждению преступности и борьбе с ней, компьютерная преступность вышла на уровень одной из международных проблем. Поэтому чрезвычайно важно добиваться эффективного решения проблем обеспечения безопасности

коммерческой информации в глобальной сети Интернет и смежных Интранет-сетях, которые по своей технической сущности не имеют принципиальных отличий и различаются в основном масштабами и открытостью.

Рассмотрим особенности стандартизации процесса обеспечения безопасности коммерческой информации в сетях с протоколом передачи данных IP/TCP и с акцентом на защиту телекоммуникаций.

Обеспечение безопасности ИТ особенно актуально для открытых систем коммерческого применения, обрабатывающих информацию ограниченного доступа, не содержащую государственную тайну. Под открытыми системами понимают совокупности всевозможного вычислительного и телекоммуникационного оборудования разного производства, совместное функционирование которого обеспечивается соответствием требованиям международных стандартов.

Термин «открытые системы» подразумевает также, что если вычислительная система соответствует стандартам, то она будет открыта для взаимосвязи с любой другой системой, которая соответствует тем же стандартам. Это, в частности, относится и к механизмам криптографической защиты информации или к защите от НСД к информации.

Важная заслуга Интернета состоит в том, что он заставил по-новому взглянуть на такие технологии. Во-первых, Интернет поощряет применение открытых стандартов, доступных для внедрения всем, кто проявит к ним интерес. Во-вторых, он представляет собой крупнейшую в мире, и вероятно, единственную, сеть, к которой подключается такое множество разных компьютеров. И наконец, Интернет становится общепринятым средством представления быстроменяющейся новой продукции и новых технологий на мировом рынке. В Интернете уже давно существует ряд комитетов, в основном из организаций-добровольцев, которые осторожно проводят предлагаемые технологии через процесс стандартизации. Эти комитеты, составляющие основную часть Рабочей группы инженеров Интернета IETF (Internet Engineering Task Force) провели стандартизацию нескольких важных протоколов, ускоряя их внедрение в Интернете. Непосредственными результатами усилий IETF являются такие протоколы, как семейство TCP/IP для передачи данных, SMTP (Simple Mail Transport Protocol) и POP (Post Office Protocol) для электронной почты, а также SNMP (Simple Network Management Protocol) для управления сетью.

В Интернете популярны протоколы безопасной передачи данных, а именно SSL, SET, IPSec. Перечисленные протоколы появились в Интернете сравнительно недавно как необходимость защиты ценной информации и сразу стали стандартами де-факто. Протокол SSL (Secure Socket Layer) – популярный сетевой протокол с шифрованием данных для безопасной передачи по сети. Он позволяет устанавливать защищенное соединение, производить контроль целостности данных и решать различные сопутствующие задачи. Протокол SSL обеспечивает защиту данных между сервисными протоколами (такими как HTTP, FTP и др.) и транспортными протоколами (TCP/IP) с помощью современной криптографии. Протокол SSL подробно рассмотрен в главе 11.

Протокол SET (Security Electronics Transaction) – перспективный стандарт безопасных электронных транзакций в сети Интернет, предназначенный для организации электронной торговли через сеть Интернет. Протокол SET основан на использовании цифровых сертификатов по стандарту X.509.

Протокол выполнения защищенных транзакций SET является стандартом, разработанным компаниями MasterCard и Visa при значительном участии IBM, GlobeSet и других партнеров. Он позволяет покупателям приобретать товары через Интернет, используя защищенный механизм выполнения платежей.

SET является открытым стандартным многосторонним протоколом для проведения безопасных платежей с использованием пластиковых карточек в Интернете. SET обеспечивает кросс-аутентификацию счета держателя карты, продавца и банка продавца для проверки готовности оплаты, а также целостность и секретность сообщения,

шифрование ценных и уязвимых данных. Поэтому SET более правильно можно назвать стандартной технологией или системой протоколов выполнения безопасных платежей с использованием пластиковых карт через Интернет. SET позволяет потребителям и продавцам подтверждать подлинность всех участников сделки, происходящей в Интернете, с помощью криптографии, в том числе применяя цифровые сертификаты.

Как упоминалось ранее, базовыми задачами защиты информации являются обеспечение ее доступности, конфиденциальности, целостности и юридической значимости. SET, в отличие от других протоколов, позволяет решать указанные задачи защиты информации в целом.

В частности, он обеспечивает следующие специальные требования защиты операций электронной коммерции:

- секретность данных оплаты и конфиденциальность информации заказа, переданной наряду с данными об оплате;
- сохранение целостности данных платежей. Целостность информации платежей обеспечивается с помощью цифровой подписи;
- специальную криптографию с открытым ключом для проведения аутентификации;
- аутентификацию держателя по кредитной карточке. Она обеспечивается применением цифровой подписи и сертификатов держателя карт;
- аутентификацию продавца и его возможности принимать платежи по пластиковым карточкам с применением цифровой подписи и сертификатов продавца;
- аутентификацию того, что банк продавца является действующей организацией, которая может принимать платежи по пластиковым карточкам через связь с процессинговой карточной системой. Аутентификация банка продавца обеспечивается использованием цифровой подписи и сертификатов банка продавца;
- готовность оплаты транзакций в результате аутентификации сертификата с открытым ключом для всех сторон;
- безопасность передачи данных посредством преимущественного использования криптографии.

Основное преимущество SET по сравнению с другими существующими системами обеспечения информационной безопасности заключается в использовании цифровых сертификатов (стандарт X509, версия 3), которые ассоциируют держателя карты, продавца и банк продавца с банковскими учреждениями платежных систем Visa и Mastercard. Кроме того, SET позволяет сохранить существующие отношения между банком, держателями карт и продавцами и интегрируется с существующими системами.

Протокол IPSec

Спецификация IPSec входит в стандарт IP v.6 и является дополнительной по отношению к текущей версии протоколов TCP/IP. Она разработана Рабочей группой IP Security IETF. В настоящее время IPSec включает 3 алгоритмо-независимых базовых спецификации, представляющих соответствующие RFC-стандарты. Протокол IPSec обеспечивает стандартный способ шифрования трафика на сетевом (третьем) уровне IP и защищает информацию на основе сквозного шифрования: независимо от работающего приложения при этом шифруется каждый пакет данных, проходящий по каналу. Это позволяет организациям создавать в Интернете виртуальные частные сети.

Инфраструктура управления открытыми ключами

Инфраструктура управления открытыми ключами PKI (Public Key Infrastructure) предназначена для защищенного управления криптографическими ключами электронного

документооборота, основанного на применении криптографии с открытыми ключами. Эта инфраструктура подразумевает использование цифровых сертификатов, удовлетворяющих рекомендациям международного стандарта X.509 и развернутой сети центров сертификации, обеспечивающих выдачу и сопровождение цифровых сертификатов для всех участников электронного обмена документами.

2. СОДЕРЖАНИЕ ОТЧЕТА

Цель работы.

Решение задания. Аналитический обзор международных стандартов по выбору преподавателя.

Ответы на контрольные вопросы.

3. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Назовите наиболее известные международные стандарты в области защиты информации.
2. Какие основные рекомендации для управления информационной безопасностью содержат руководства Британского института стандартов — British Standards Institution (BSI)?
3. Какие основные критерии безопасности информационных технологий изложены в Международном стандарте ISO 15408?
4. Какие организации приняли участие в разработке международного стандарта по критериям оценки безопасности ИТ для общего использования?
5. Какие стандарты для беспроводных сетей вам известны?
6. Какие стандарты информационной безопасности в Интернете вам известны?

СПИСОК ИСТОЧНИКОВ

Основная литература:

1. [Электрон, ресурс] – http://ypn.ru/177/international-standards-of-information-technologies-security/ Your Private Network (Лаборатория Сетевой Безопасности)