Белорусско-Российский университет
Кафедра «Программное обеспечение информационных технологий»

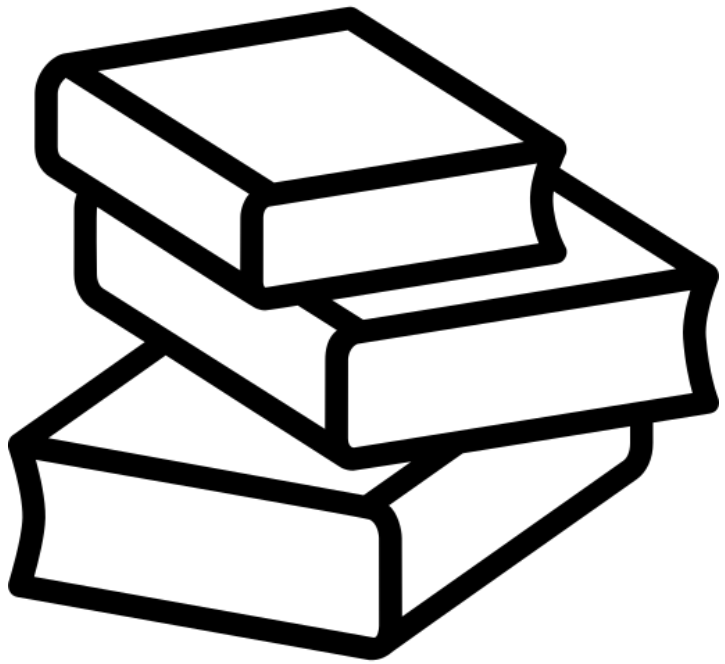
Защита информации

Правовое и нормативное обеспечение защиты информации

(Законодательство РБ)

КУТУЗОВ Виктор Владимирович

Республика Беларусь, Могилев, 2024



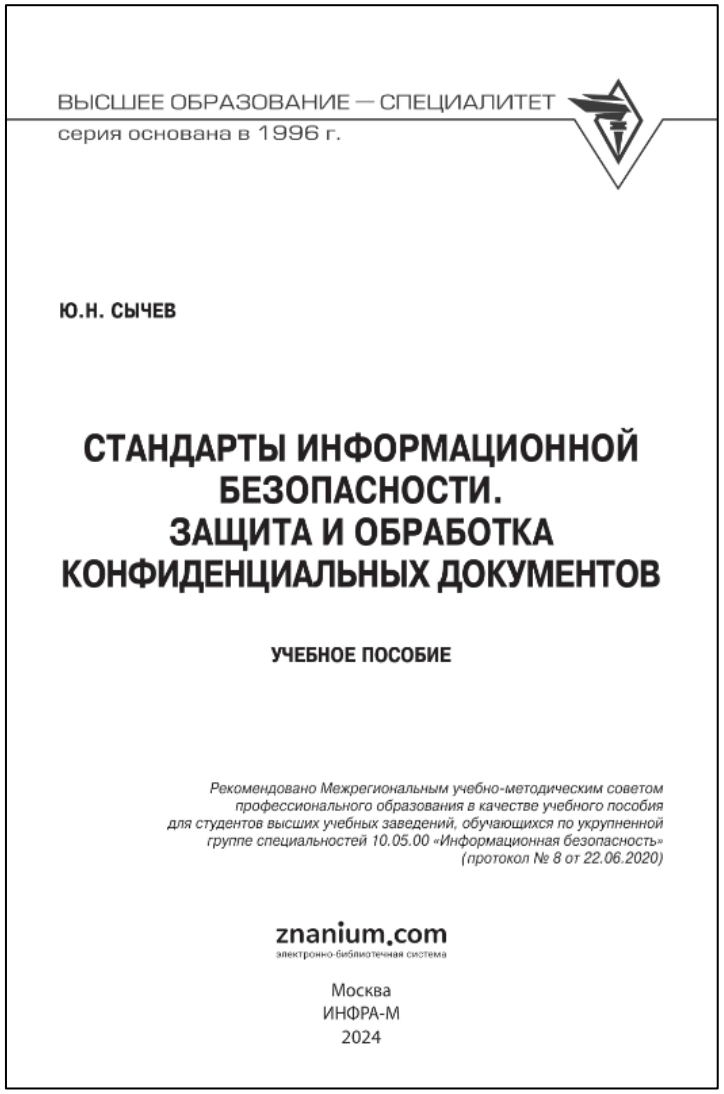
Рекомендуемая литература по теме

Рекомендуемая литература по теме

Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2023. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1912992

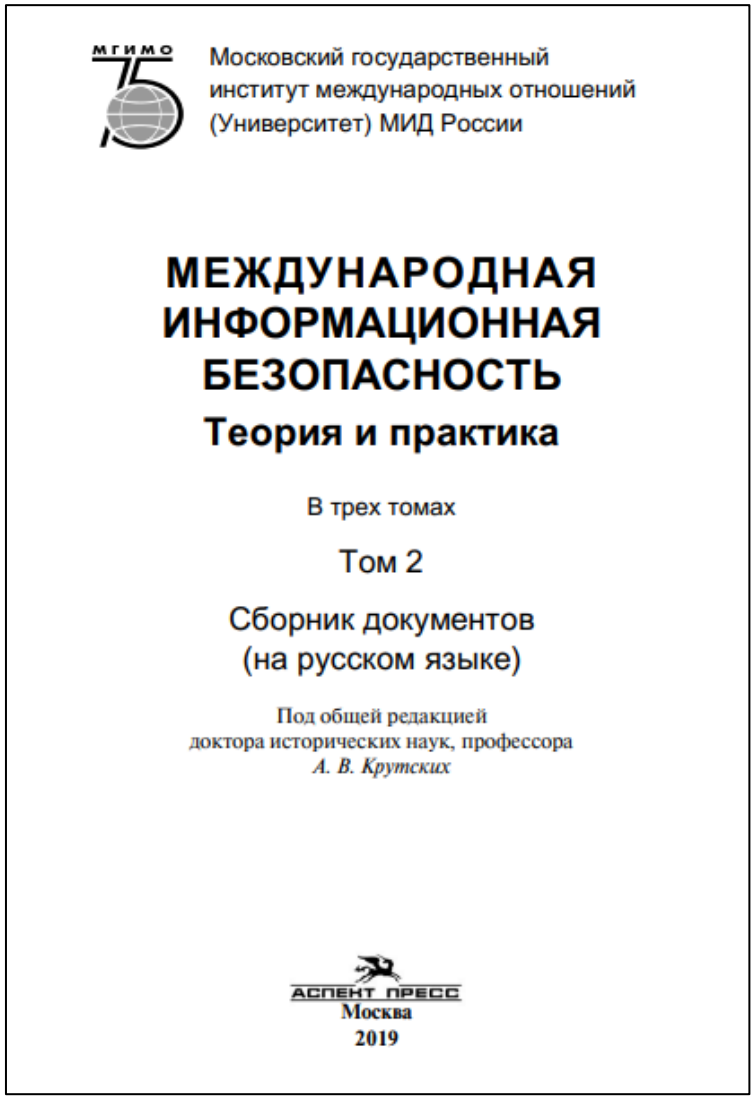
Стр. 63-98 - Глава 2 Правовое обеспечение защиты информации

Рекомендуемая литература по теме



Сычев, Ю. Н. **Стандарты информационной безопасности. Защита и обработка конфиденциальных документов** : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2024. — 223 с. — (Высшее образование: Специалитет). - ISBN 978-5-16-016533-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/2003474

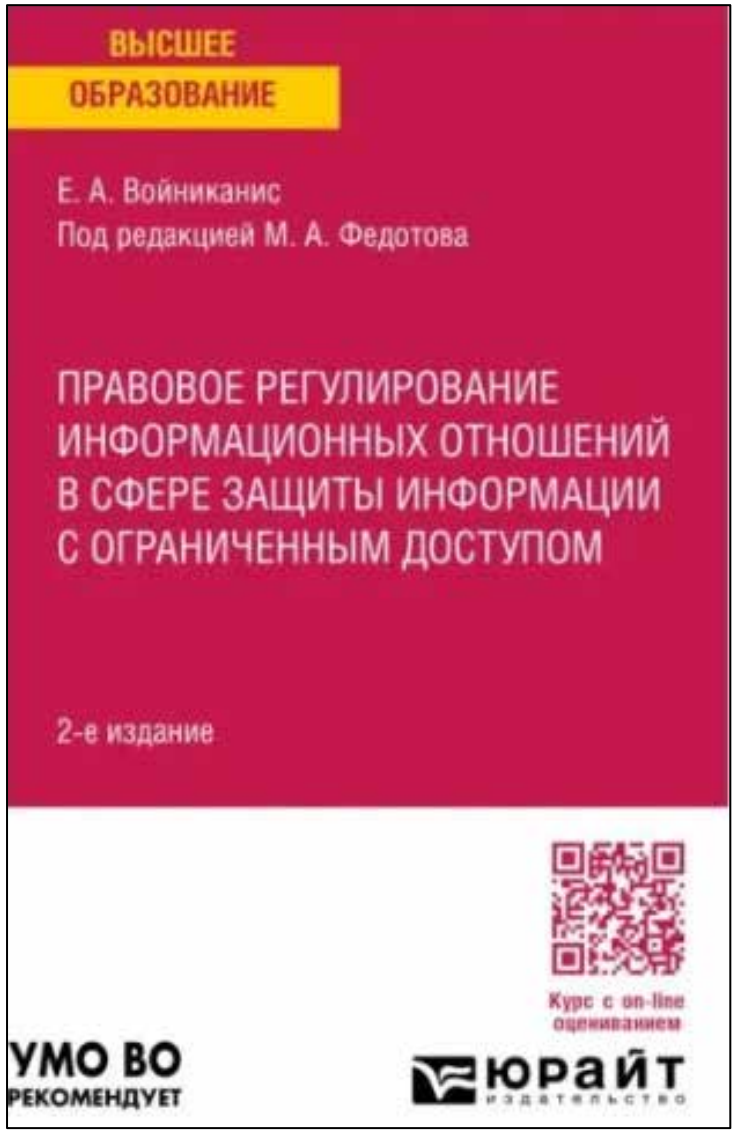
Рекомендуемая литература по теме



Международная информационная безопасность: Теория и практика: В трех томах. Том 2: Сборник документов (на русском языке) / Под общ. ред. А. В. Крутских. — М.: Издательство «Аспект Пресс», 2019.— 784 с. https://mgimo.ru/upload/iblock/559/Tom%202.pdf

Международное законодательство

Рекомендуемая литература по теме



Войниканис, Е. А. **Правовое регулирование информационных отношений в сфере защиты информации с ограниченным доступом** : учебное пособие для вузов / Е. А. Войниканис ; под редакцией М. А. Федотова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 57 с. — (Высшее образование). — ISBN 978-5-534-17204-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/532605

Законодательство РФ

Комплексный подход к обеспечению защиты объектов информационной безопасности

Комплексный подход к обеспечению защиты объектов информационной безопасности

Программно-технические методы защиты информации, какими бы совершенными они ни были, в полном объеме не решают задач комплексной защиты объектов информационной безопасности. Используемые при этом физические, аппаратные, программные, криптографические и иные логические и технические средства и методы защиты выполняются без участия человека по заранее предусмотренной процедуре.

Для обеспечения комплексного подхода к обеспечению защиты объектов информационной безопасности должны быть соответствующие правовые акты, устанавливающие порядок защиты и ответственность за его нарушение.

Классификация методов защиты информации

Правовые методы защиты информации

- Правовое обеспечение защиты информации (ЗИ):

- **Нормотворческая деятельность**
  - Создание законодательства в области информационной безопасности

- **Исполнительная и правоприменительная деятельность**
  - Контроль за исполнением законодательства государственными органами, организациями и гражданами

Нормотворческая деятельность

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

Исполнительная и правоприменительная деятельность

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

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

Фундаментальные положения правового обеспечения информационной безопасности

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

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

Законодательство в области информационной безопасности

В каждой стране действует законодательство в области информационной безопасности в рамках которого обязаны работать компании.

2.1. Законодательная база Республики Беларусь

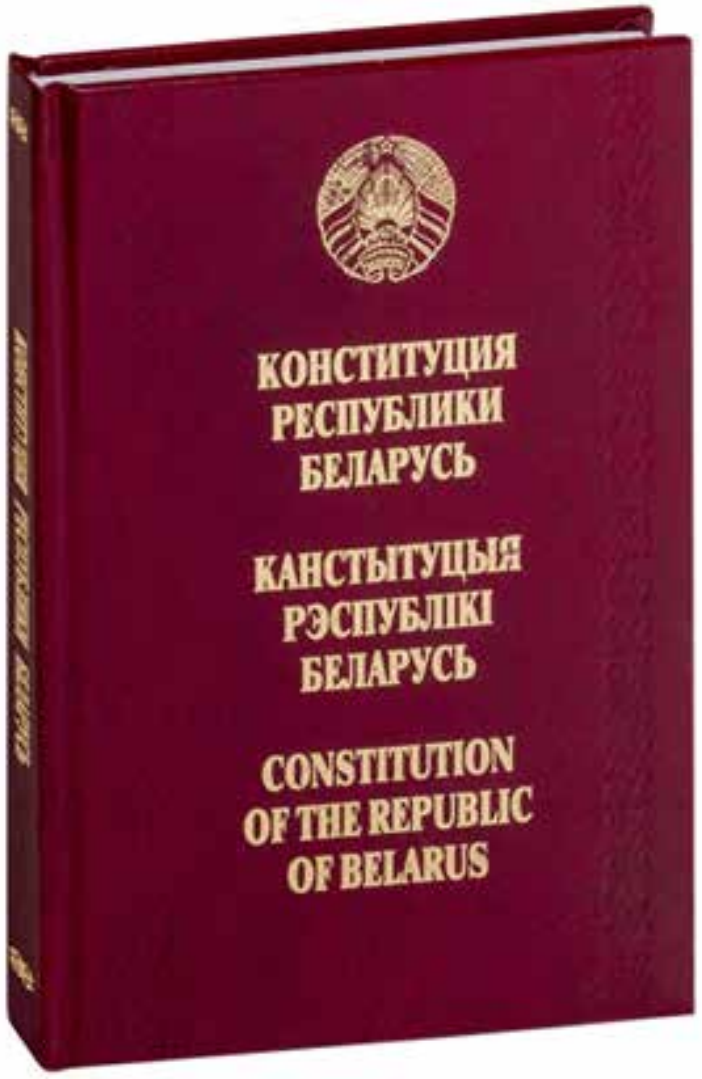
Основные правовые акты, регламентирующие защиту информации в РБ

- Конституция Республики Беларусь
- Концепция национальной безопасности РБ
- Концепция информационной безопасности РБ
- Указ «О кибербезопасности»
- Закон «О защите персональных данных»
- Закон «Об информации, информатизации и защите информации»
- Закон «О государственных секретах»
- Закон «Об электронном документе и электронной цифровой подписи»
- и многие другие законы, указы, постановления и распоряжения

Организации

- Оперативно-аналитический центр при Президенте Республики Беларусь
- Национальный центр защиты персональных данных Республики Беларусь
- Комитет государственной безопасности
- Министерство внутренних дел Республики Беларусь
- Национальная команда реагирования на киберинциденты
- Центры обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций
- и многие другие

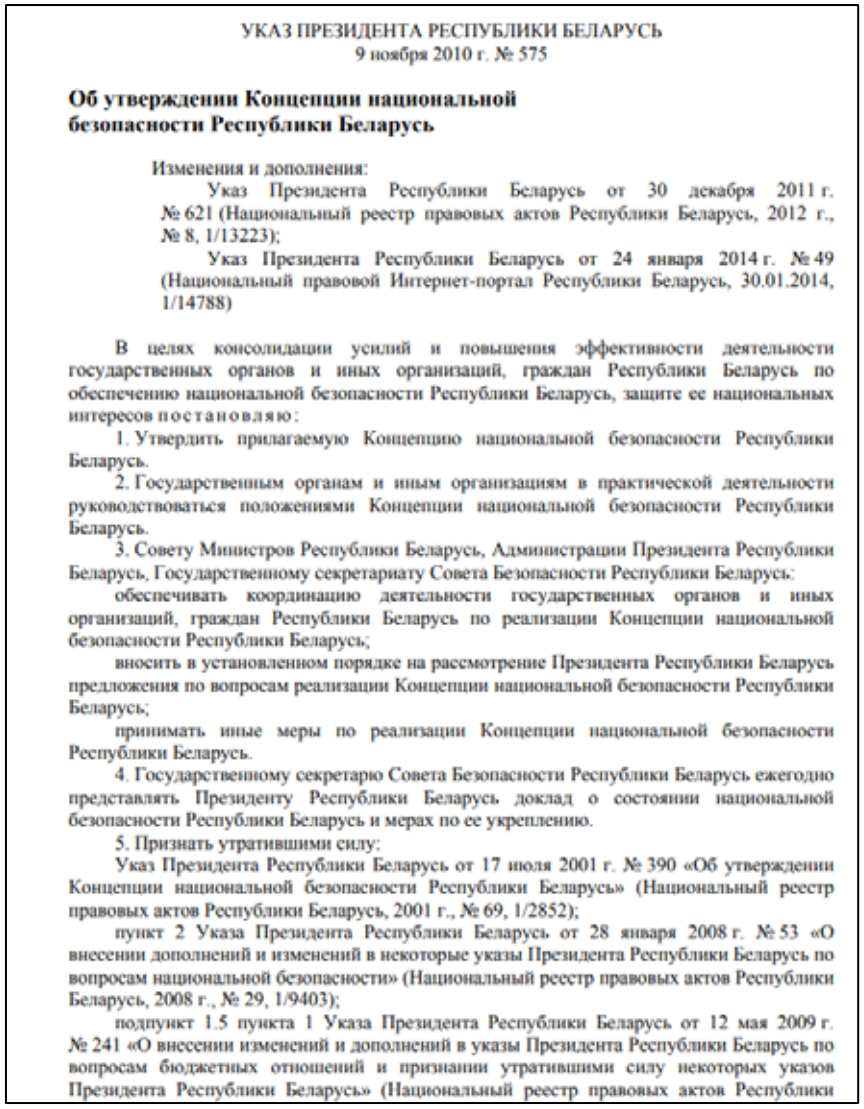
Конституция Республики Беларусь



- **Статья 34.** 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.
- Государственные органы, общественные объединения, должностные лица обязаны предоставить гражданину Республики Беларусь возможность ознакомиться с материалами, затрагивающими его права и законные интересы.
- **Пользование информацией может быть ограничено законодательством** в целях защиты чести, достоинства, личной и семейной жизни граждан и полного осуществления ими своих прав.

https://pravo.by/pravovaya-informatsiya/normativnye-dokumenty/konstitutsiya-respubliki-belarus/

КОНЦЕПЦИЯ национальной безопасности Республики Беларусь (2010)



УКАЗ ПРЕЗИДЕНТА РЕСПУБЛИКИ БЕЛАРУСЬ
9 ноября 2010 г. № 575

Об утверждении Концепции национальной безопасности Республики Беларусь

Изменения и дополнения:
Указ Президента Республики Беларусь от 30 декабря 2011 г. № 621 (Национальный реестр правовых актов Республики Беларусь, 2012 г., № 8, 1/13223);
Указ Президента Республики Беларусь от 24 января 2014 г. № 49 (Национальный правовой Интернет-портал Республики Беларусь, 30.01.2014, 1/14788)

В целях консолидации усилий и повышения эффективности деятельности государственных органов и иных организаций, граждан Республики Беларусь по обеспечению национальной безопасности Республики Беларусь, защите ее национальных интересов постановляю:

1. Утвердить прилагаемую Концепцию национальной безопасности Республики Беларусь.

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

3. Совету Министров Республики Беларусь, Администрации Президента Республики Беларусь, Государственному секретариату Совета Безопасности Республики Беларусь:

обеспечивать координацию деятельности государственных органов и иных организаций, граждан Республики Беларусь по реализации Концепции национальной безопасности Республики Беларусь;

вносить в установленном порядке на рассмотрение Президента Республики Беларусь предложения по вопросам реализации Концепции национальной безопасности Республики Беларусь;

принимать иные меры по реализации Концепции национальной безопасности Республики Беларусь.

4. Государственному секретарю Совета Безопасности Республики Беларусь ежегодно представлять Президенту Республики Беларусь доклад о состоянии национальной безопасности Республики Беларусь и мерах по ее укреплению.

5. Признать утратившими силу:

Указ Президента Республики Беларусь от 17 июля 2001 г. № 390 «Об утверждении Концепции национальной безопасности Республики Беларусь» (Национальный реестр правовых актов Республики Беларусь, 2001 г., № 69, 1/2852);

пункт 2 Указа Президента Республики Беларусь от 28 января 2008 г. № 53 «О внесении дополнений и изменений в некоторые указы Президента Республики Беларусь по вопросам национальной безопасности» (Национальный реестр правовых актов Республики Беларусь, 2008 г., № 29, 1/9403);

подпункт 1.5 пункта 1 Указа Президента Республики Беларусь от 12 мая 2009 г. № 241 «О внесении изменений и дополнений в указы Президента Республики Беларусь по вопросам бюджетных отношений и признании утратившими силу некоторых указов Президента Республики Беларусь» (Национальный реестр правовых актов Республики

- Настоящая Концепция закрепляет совокупность официальных взглядов на сущность и содержание деятельности Республики Беларусь по обеспечению баланса интересов личности, общества, государства и их защите от внутренних и внешних угроз.
- В концепции большое внимание уделяется информационной безопасности, внутренним и внешним информационным угрозам, вопросам информационной политике.

Указ Президента Республики Беларусь от 9 ноября 2010 г. № 575 КОНЦЕПЦИЯ национальной безопасности Республики Беларусь
https://pravo.by/document/?guid=3871&p0=P31000575

КОНЦЕПЦИЯ национальной безопасности Республики Беларусь (2010)

- **14. Основными национальными интересами в информационной сфере являются:**

1. реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации;
2. формирование и поступательное развитие информационного общества;
3. равноправное участие Республики Беларусь в мировых информационных отношениях;
4. преобразование информационной индустрии в экспортно-ориентированный сектор экономики;
5. эффективное информационное обеспечение государственной политики;
6. обеспечение надежности и устойчивости функционирования критически важных объектов информатизации.

Проект новой Концепции национальной безопасности Республики Беларусь (2023)

- **Информационная сфера становится ареной межгосударственного противостояния.** В результате культурно-идеологической экспансии, в основном ориентированной на потребление, целенаправленно искажается историческая правда, осуществляется фальсификация истории, разрушаются культурное наследие человечества, традиционные духовно-нравственные ценности народов, их национальная идентичность, институт семьи и пространство межкультурного взаимодействия. Электронные средства массовой коммуникации оказывают всеобъемлющее влияние на общественно-политические и социально-экономические процессы, используются для провоцирования внутренних конфликтов и разрушения государств.
- В условиях глобальной цифровизации кибербезопасность критической инфраструктуры и больших данных приобрела исключительное значение для обеспечения устойчивости всех сфер жизнедеятельности. Расширяется круг государств, создающих силы обеспечения информационной безопасности, в том числе кибервойска, в задачи которых входит проведение операций в информационной сфере.

https://pravo.by/document/?guid=3871&p0=P223s0001

Проект новой Концепции национальной безопасности Республики Беларусь (2023)

- **15. Основными национальными интересами в информационной сфере являются:**

1. реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации;
2. сохранение национальной идентичности и памяти о героическом прошлом белорусского народа;
3. дальнейшее развитие безопасной информационной среды и информационного общества;
4. защита общества от деструктивного информационного воздействия;
5. преобразование информационной индустрии в экспортно-ориентированный сектор экономики;
6. эффективное информационное обеспечение и сопровождение государственной политики;
7. надежное и устойчивое функционирование национальных информационных систем и инфраструктуры, ресурсов субъектов информационных отношений;
8. развитие международного информационного сотрудничества на основе национальных интересов Республики Беларусь;
9. обеспечение сохранности государственных секретов и иной информации, распространение и (или) представление которой ограничено.

https://pravo.by/document/?guid=3871&p0=P223s0001

Проект новой Концепции национальной безопасности Республики Беларусь (2023)

- **37. В информационной сфере внутренними источниками угроз национальной безопасности являются:**
- распространение недостоверной или умышленно искаженной информации, способной причинить вред национальным интересам Республики Беларусь;
- зависимость Республики Беларусь от импорта информационных технологий, средств информатизации и защиты информации, неконтролируемое их использование в системах, отказ или разрушение которых может причинить вред национальной безопасности;
- несоответствие качества национального контента мировому уровню;
- активное использование информационно-коммуникационных технологий для совершения правонарушений;
- расширение возможностей для неправомерных действий в отношении персональных данных;
- недостаточная эффективность информационного обеспечения государственной политики;
- низкий уровень правосознания и безопасного поведения пользователей информационно-коммуникационных технологий;
- нарушение установленного порядка обращения с государственными секретами.

https://pravo.by/document/?guid=3871&p0=P223s0001

Проект новой Концепции национальной безопасности Республики Беларусь (2023)

- **46. В информационной сфере внешними источниками угроз национальной безопасности являются:**
- доминирование ведущих зарубежных государств в мировом информационном пространстве, монополизация ключевых сегментов информационных рынков зарубежными информационными структурами;
- целенаправленная деятельность зарубежных государств, международных и иных организаций, отдельных лиц, наносящая вред национальным интересам Республики Беларусь в информационной сфере, в первую очередь по формированию негативного образа государства в мире;
- нарастание информационного противоборства между ведущими мировыми центрами силы, подготовка и ведение зарубежными государствами борьбы в информационном пространстве;
- препятствование распространению национального контента Республики Беларусь за рубежом;
- широкое распространение в мировом информационном пространстве образцов массовой культуры, противоречащих общечеловеческим и национальным духовно-нравственным ценностям;
- несовершенство механизмов международного сотрудничества в противодействии преступности с использованием информационно-коммуникационных технологий.

https://pravo.by/document/?guid=3871&p0=P223s0001

Проект новой Концепции национальной безопасности Республики Беларусь (2023)

- **Важнейшими направлениями нейтрализации внутренних источников угроз национальной безопасности в информационной сфере являются:**
- обеспечение защиты персональных данных от несанкционированного или случайного доступа к ним, иных неправомерных действий;
- противодействие деструктивному информационному воздействию, наносящему вред национальным интересам;
- информационное обеспечение и сопровождение государственной политики, в том числе информационное противоборство для защиты информационного пространства;
- развитие массового политического сознания граждан;
- усиление позитивного восприятия Беларуси в мировом информационном пространстве;
- дальнейшая реализация стратегии по формированию в Республике Беларусь информационного общества, гарантированное обеспечение установленного законодательством порядка доступа к государственным информационным ресурсам, в том числе удаленного, получение информационных услуг;
- динамичное внедрение информационно-коммуникационных и передовых производственных технологий в отрасли национальной экономики и сферы жизнедеятельности общества, в том числе методов и средств защиты информации в информационных системах, используемых в инфраструктуре, являющейся жизненно важной для страны;
- создание комплексной цифровой инфраструктуры для межведомственного информационного взаимодействия;
- формирование современной системы оказания государственных услуг на принципах проактивности и мультиканальности их предоставления;
- развитие национальной системы обеспечения кибербезопасности;
- профилактика, выявление и пресечение правонарушений, совершаемых с использованием информационно-коммуникационных технологий;
- совершенствование системы защиты информации и сведений, составляющих охраняемую законодательством тайну.

https://pravo.by/document/?guid=3871&p0=P223s0001

Проект новой Концепции национальной безопасности Республики Беларусь (2023)

- **Меры по защите от внешних источников угроз национальной безопасности в информационной сфере осуществляются путем:**
- участия Республики Беларусь в формировании механизмов международного и регионального сотрудничества по противодействию преступности с использованием информационно-коммуникационных технологий исходя из национальных интересов;
- создания и безопасного использования межгосударственных, международных глобальных информационных сетей и систем;
- сокращения использования иностранных информационных технологий.

https://pravo.by/document/?guid=3871&p0=P223s0001

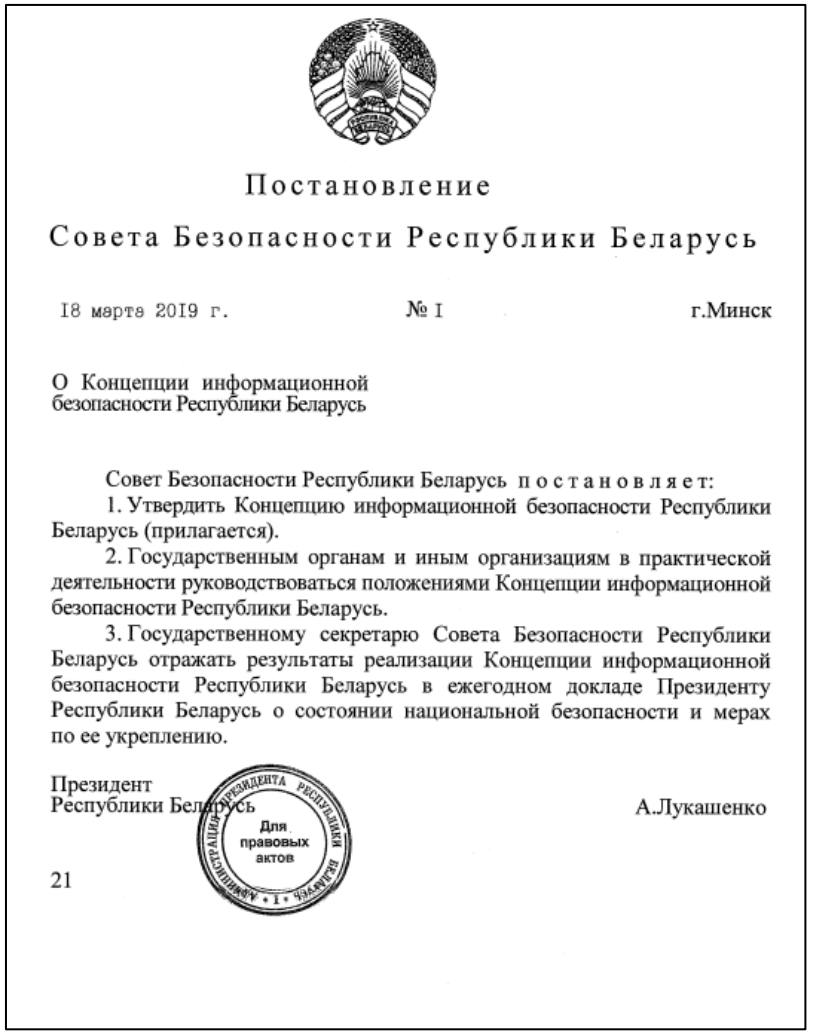
Проект новой Концепции национальной безопасности Республики Беларусь (2023)

- **Решение задач обеспечения национальной безопасности осуществляется на основе системной реализации комплекса взаимосвязанных политических, дипломатических, экономических, правовых, военных, информационных и иных средств**, направленных на выявление, предупреждение и нейтрализацию внутренних и внешних рисков, вызовов и угроз безопасности личности, общества и государства, а также на упреждение либо минимизацию масштабов нанесения вреда национальным интересам Республики Беларусь.
- Степень концентрации и объем использования имеющихся ресурсов определяются исходя из вероятности и степени воздействия конкретных угроз на Республику Беларусь, а также реальных возможностей государства и общества.

https://pravo.by/document/?guid=3871&p0=P223s0001

Постановление Совета Безопасности Республики Беларусь 18.03.2019 № 1

Концепция информационной безопасности Республики Беларусь



Постановление

Совета Безопасности Республики Беларусь

18 марта 2019 г. № 1 г.Минск

О Концепции информационной безопасности Республики Беларусь

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

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

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

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

Президент Республики Беларусь А.Лукашенко

Для правовых актов

21

- **Концепция информационной безопасности Беларуси** – это система официальных взглядов на сущность и содержание обеспечения национальной безопасности в информационной сфере, в которой определяются стратегические задачи и приоритеты в области обеспечения информационной безопасности.
- Документ обеспечивает комплексный подход к проблеме информационной безопасности, создает методологическую основу для совершенствования деятельности по ее укреплению, служит основанием для формирования государственной политики, выработки мер по совершенствованию системы обеспечения информационной безопасности, конструктивного взаимодействия, консолидации усилий и повышения эффективности защиты национальных интересов в информационной сфере, способствует целенаправленной интеграции Беларуси в системы обеспечения международной информационной безопасности на основе национальных приоритетов.
- В Концепции отражены современные вызовы и угрозы, которые формируются в информационной сфере и представляют опасность для конституционных основ и жизнедеятельности государств - манипулирование массовым сознанием, дискредитация идеалов и ценностей, размывание национального суверенитета, неустойчивость информационной инфраструктуры и другие.
- http://mininform.gov.by/upload/medialibrary/6f8/6f80a36dcb2aac3bcaa330cda20ae733.pdf
- https://pravo.by/document/?guid=3871&p0=P219s0001

Концепция информационной безопасности Союзного государства

ПОСТАНОВЛЕНИЕ ВЫСШЕГО ГОСУДАРСТВЕННОГО СОВЕТА
СОЮЗНОГО ГОСУДАРСТВА

22 февраля 2023 г. № 1

г. Минск

О Концепции информационной безопасности Союзного государства

Высший Государственный Совет Союзного государства ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемую Концепцию информационной безопасности Союзного государства.

2. Настоящее постановление вступает в силу со дня его подписания.

КОНЦЕПЦИЯ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОЮЗНОГО ГОСУДАРСТВА

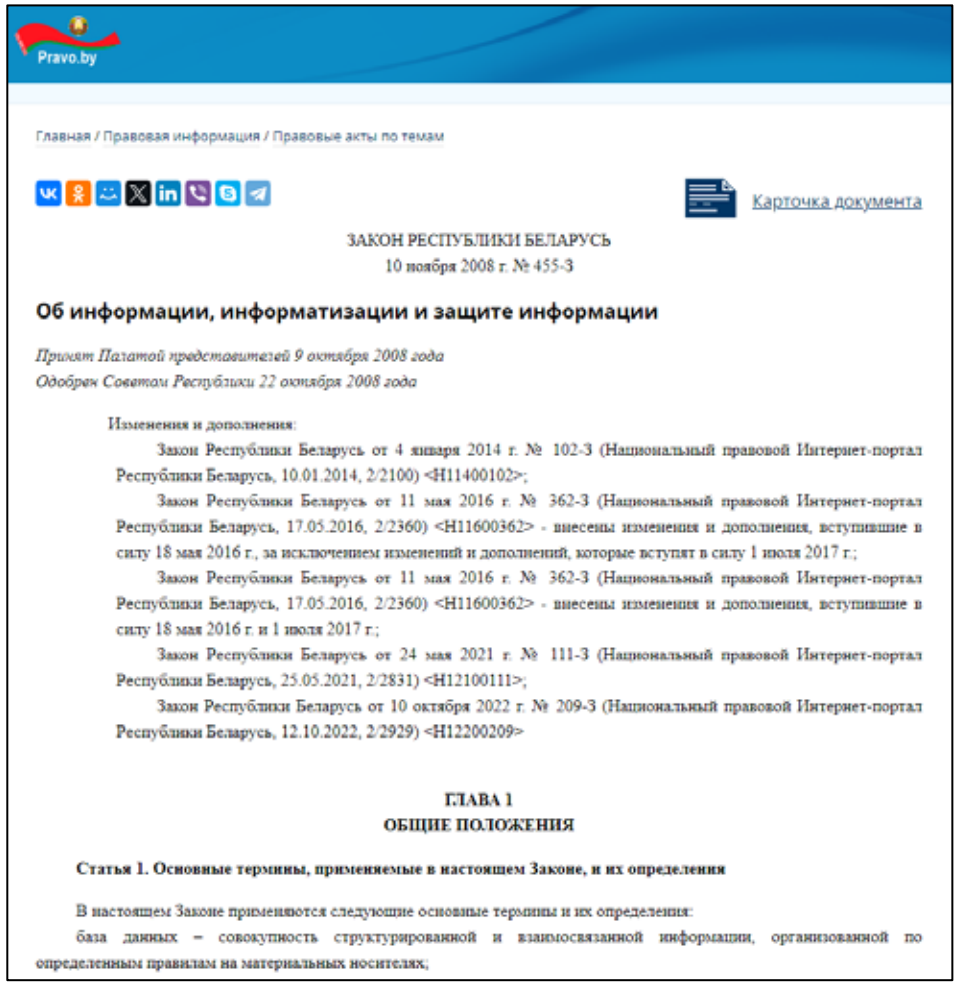
I. Общие положения

1. Концепция информационной безопасности Союзного государства (далее – Концепция) – система официально принятых в Российской Федерации и Республике Беларусь взглядов на обеспечение информационной безопасности Союзного государства.

2. Правовую основу настоящей Концепции составляют Конституция Российской Федерации и Конституция Республики Беларусь, Договор о создании Союзного государства от 8 декабря 1999 года, законодательные и другие нормативные правовые акты Российской Федерации и Республики Беларусь (далее – национальные законодательства) в области обеспечения национальной безопасности в информационной сфере.

- **Концепция определяет основы для формирования согласованной государственной политики и развития общественных отношений в области обеспечения информационной безопасности**, а также выработки мер по совершенствованию систем обеспечения информационной безопасности государств – участников Договора о создании Союзного государства.
- Документ способствует повышению защищенности информационной инфраструктуры государств-участников и, прежде всего, их критически важных объектов, а также нацелен на борьбу с деструктивным воздействием на информационные ресурсы Союзного государства.

Закон «Об информации, информатизации и защите информации»



Pravo.by

Главная / Правовая информация / Правовые акты по темам

Карточка документа

ЗАКОН РЕСПУБЛИКИ БЕЛАРУСЬ
10 ноября 2008 г. № 455-З

Об информации, информатизации и защите информации

Принят Палатой представителей 9 октября 2008 года
Одобрен Советом Республики 22 октября 2008 года

Изменения и дополнения:

Закон Республики Беларусь от 4 января 2014 г. № 102-З (Национальный правовой Интернет-портал Республики Беларусь, 10.01.2014, 2/2100) <H11400102>;

Закон Республики Беларусь от 11 мая 2016 г. № 362-З (Национальный правовой Интернет-портал Республики Беларусь, 17.05.2016, 2/2360) <H11600362> - внесены изменения и дополнения, вступившие в силу 18 мая 2016 г., за исключением изменений и дополнений, которые вступят в силу 1 июля 2017 г.;

Закон Республики Беларусь от 11 мая 2016 г. № 362-З (Национальный правовой Интернет-портал Республики Беларусь, 17.05.2016, 2/2360) <H11600362> - внесены изменения и дополнения, вступившие в силу 18 мая 2016 г. и 1 июля 2017 г.;

Закон Республики Беларусь от 24 мая 2021 г. № 111-З (Национальный правовой Интернет-портал Республики Беларусь, 25.05.2021, 2/2831) <H12100111>;

Закон Республики Беларусь от 10 октября 2022 г. № 209-З (Национальный правовой Интернет-портал Республики Беларусь, 12.10.2022, 2/2929) <H12200209>

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;

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, защитой детей от информации, причиняющей вред их здоровью и развитию, научно-технической, статистической, правовой, экологической и иной информацией.

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

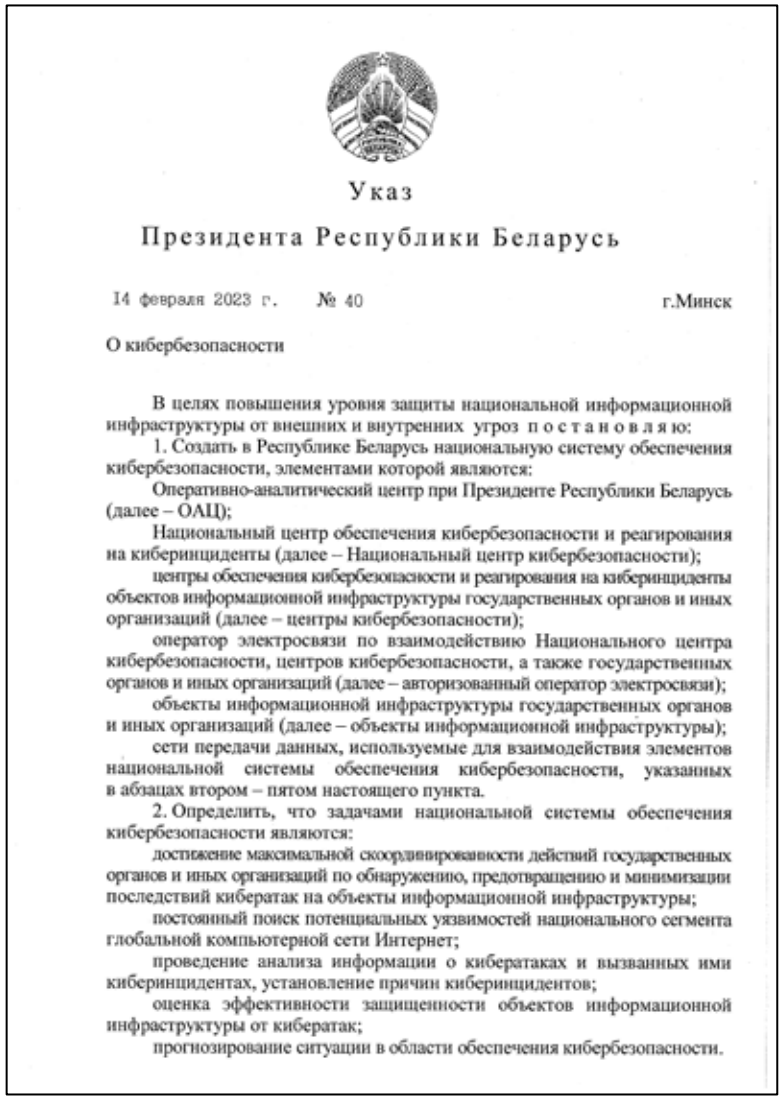
Закон Республики Беларусь от 10 ноября 2008 г. № 455-З
Об информации, информатизации и защите информации
https://pravo.by/document/?guid=3871&p0=h10800455

Закон «Об информации, информатизации и защите информации»

- В законе **приводятся:**
  - **полномочия различных государственных органов** в области информации, информатизации и защиты информации;
  - **виды информации** и возможности её распространения;
  - **виды информационных ресурсов и систем** и их Государственная регистрация;
  - **требования по защите информации**;
  - **права и обязанности** субъектов информационных отношений;
  - **ответственность** за нарушение требований законодательства об информации, информатизации и защите информации;

Закон Республики Беларусь от 10 ноября 2008 г. № 455-З Об информации, информатизации и защите информации
https://pravo.by/document/?guid=3871&p0=h10800455

Указ № 40 от 14 февраля 2023
О кибербезопасности



Указ

Президента Республики Беларусь

14 февраля 2023 г. № 40 г.Минск

О кибербезопасности

В целях повышения уровня защиты национальной информационной инфраструктуры от внешних и внутренних угроз п о с т а н о в л я ю:

1. Создать в Республике Беларусь национальную систему обеспечения кибербезопасности, элементами которой являются:

Оперативно-аналитический центр при Президенте Республики Беларусь (далее – ОАЦ);

Национальный центр обеспечения кибербезопасности и реагирования на кибериндиденты (далее – Национальный центр кибербезопасности);

центры обеспечения кибербезопасности и реагирования на кибериндиденты объектов информационной инфраструктуры государственных органов и иных организаций (далее – центры кибербезопасности);

оператор электросвязи по взаимодействию Национального центра кибербезопасности, центров кибербезопасности, а также государственных органов и иных организаций (далее – авторизованный оператор электросвязи);

объекты информационной инфраструктуры государственных органов и иных организаций (далее – объекты информационной инфраструктуры);

сети передачи данных, используемые для взаимодействия элементов национальной системы обеспечения кибербезопасности, указанных в абзацах втором – пятом настоящего пункта.

2. Определить, что задачами национальной системы обеспечения кибербезопасности являются:

достижение максимальной скоординированности действий государственных органов и иных организаций по обнаружению, предотвращению и минимизации последствий кибератак на объекты информационной инфраструктуры;

постоянный поиск потенциальных уязвимостей национального сегмента глобальной компьютерной сети Интернет;

проведение анализа информации о кибератаках и вызванных ими киберинцидентах, установление причин киберинцидентов;

оценка эффективности защищенности объектов информационной инфраструктуры от кибератак;

прогнозирование ситуации в области обеспечения кибербезопасности.

Указ № 40 от 14 февраля 2023 г. «О кибербезопасности»

Документом определяется правовая основа создания и функционирования национальной системы обеспечения кибербезопасности, предусматривающей формирование комплексного многоуровневого механизма противодействия кибератакам на государственные органы и организации, критическую информационную инфраструктуру. В частности, конкретизированы функции и задачи по обеспечению кибербезопасности государственных органов и иных организаций, закреплена персональная ответственность их руководителей, а также определены владельцы критически важных объектов информатизации, обеспечивающие первоочередное создание центров кибербезопасности.

Указ направлен на дальнейшую реализацию положений Концепции национальной безопасности и взаимосвязан с Концепцией информационной безопасности.

Реализация мер, предусмотренных в Указе, позволит консолидировать усилия по предотвращению, обнаружению и минимизации последствий кибератак на объекты информационной инфраструктуры, тем самым повысить безопасность и надежность информационных систем.

https://president.gov.by/ru/documents/ukaz-no-40-ot-14-fevralya-2023-g
https://president.gov.by/bucket/assets/uploads/documents/2023/40uk.pdf

Указ № 40 от 14 февраля 2023

О кибербезопасности

- **Кибербезопасность** – состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз.

- **Киберинцидент** – событие, которое фактически или потенциально угрожает конфиденциальности, целостности, подлинности, доступности и сохранности информации, а также представляет собой нарушение (угрозу нарушения) политики безопасности.

Указ № 40 от 14 февраля 2023

О кибербезопасности

- **Кибератака** – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

- **Информационная инфраструктура** – совокупность технических средств, систем и технологий создания, преобразования, передачи, использования и хранения информации.

Указ № 40 от 14 февраля 2023

О кибербезопасности

- **В Республике Беларусь создается национальная система обеспечения кибербезопасности, элементами которой являются:**
  - Оперативно-аналитический центр при Президенте Республики Беларусь (**ОАЦ**);
  - Национальный центр обеспечения кибербезопасности и реагирования на киберинциденты (**Национальный центр кибербезопасности**);
  - центры обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций (**центры кибербезопасности**);
  - оператор электросвязи по взаимодействию Национального центра кибербезопасности, центров кибербезопасности, а также государственных органов и иных организаций (**авторизованный оператор электросвязи**);
  - объекты информационной инфраструктуры государственных органов и иных организаций (**объекты информационной инфраструктуры**);
  - **сети передачи данных**, используемые для взаимодействия элементов национальной системы обеспечения кибербезопасности.

Указ № 40 от 14 февраля 2023

О кибербезопасности

- **Задачами национальной системы обеспечения кибербезопасности являются:**
  - **достижение максимальной скоординированности действий** государственных органов и иных организаций по обнаружению, предотвращению и минимизации последствий кибератак на объекты информационной инфраструктуры;
  - **постоянный поиск потенциальных уязвимостей** национального сегмента глобальной компьютерной сети Интернет;
  - **проведение анализа информации о кибератаках** и вызванных ими киберинцидентах, установление причин киберинцидентов;
  - **оценка эффективности защищенности объектов** информационной инфраструктуры от кибератак;
  - **прогнозирование ситуации** в области обеспечения кибербезопасности.

Указ № 40 от 14 февраля 2023

О кибербезопасности

- **Уполномоченные лица Национального центра кибербезопасности будут вправе требовать** от государственных органов и иных организаций:
  - **представления документов (их копий) и (или) иной информации**, в том числе технического характера, связанных с функционированием принадлежащих им объектов информационной инфраструктуры. Такие документы (их копии), иная информация должны быть представлены не позднее дня, следующего за днем предъявления требования об их представлении;
  - **обеспечения беспрепятственного доступа** в помещения и иные объекты, в которых размещены объекты информационной инфраструктуры, а также к программно-техническим средствам (в том числе удаленно), с помощью которых обеспечивается их функционирование.

- Уполномоченные лица организаций, которые оказывают услуги по обеспечению кибербезопасности объектов информационной инфраструктуры, обладают такими же правами лишь в том случае, если они определены в договоре на оказание услуг по обеспечению кибербезопасности.

Указ № 40 от 14 февраля 2023

О кибербезопасности

Персональная ответственность за обеспечение кибербезопасности государственного органа и иной организации **возложена** Указом **на руководителя** этого органа (организации).

Указ № 40 от 14 февраля 2023

О кибербезопасности

- В организации может быть назначен **заместитель руководителя по вопросам обеспечения кибербезопасности**

- Основное требования к заместителю - высшее образование в области защиты информации либо повышение квалификации по вопросам обеспечения кибербезопасности на базе республиканского унитарного предприятия «Национальный центр обмена трафиком».

Рекомендации по определению прав и обязанностей заместителя руководителя государственного органа и иной организации
https://www.oac.gov.by/activity/cybersecurity-centers-list/recommendations-determining-rights

Обязанности заместителя руководителя по вопросам обеспечения кибербезопасности

- организации соблюдения требований нормативных правовых и локальных правовых актов в области обеспечения кибербезопасности;
- организации разработки, согласования и утверждения локальных правовых актов по вопросам обеспечения кибербезопасности в государственном органе (организации), в том числе политики безопасности, направленной на обеспечение стабильной деятельности государственного органа (организации) в случае проведения кибератак;
- организации контроля за состоянием кибербезопасности в государственном органе (организации);
- организации обучения работников государственного органа (организации) по вопросам обеспечения кибербезопасности;
- совершенствованию деятельности по обеспечению кибербезопасности в государственном органе (организации);
- организации информационного взаимодействия с другими элементами национальной системы обеспечения кибербезопасности;
- обеспечению уполномоченным лицам Национального центра кибербезопасности и центра кибербезопасности, обеспечивающего кибербезопасность объектов информационной инфраструктуры этого государственного органа (организации), беспрепятственного доступа в помещения и на иные объекты (на территории), где размещены (функционируют) объекты информационной инфраструктуры, а также к программно-техническим средствам (в том числе удаленно), с помощью которых обеспечивается их функционирование;
- организации порядка взаимодействия структурных подразделений государственного органа (организации) при решении вопросов обеспечения кибербезопасности.

Заместитель руководителя по вопросам обеспечения кибербезопасности обязан знать

- содержание нормативных правовых актов Республики Беларусь и локальных правовых актов государственного органа (организации), международных и национальных стандартов в области обеспечения кибербезопасности, в том числе требований по кибербезопасности, предъявляемых к объектам информационной инфраструктуры государственных органов (организаций);
- цели, задачи, основы организации, основные способы и средства обеспечения кибербезопасности в контексте основных процессов функционирования государственного органа (организации);
- уровень влияния информационных технологий на деятельность государственного органа (организации), в том числе их роль и место в процессах функционирования государственного органа (организации);
- общие сведения о способах построения информационных систем и сетей, их типовых архитектурах, применяемых средствах вычислительной техники, сетевом оборудовании, системном и прикладном программном обеспечении, системах управления базами данных, средствах технической и криптографической защиты информации, в том числе используемых и(или) применяемых в этом государственном органе (организации);
- возможные варианты реализации и контроля достижения целей обеспечения кибербезопасности государственного органа (организации);
- основные негативные последствия киберинцидентов, которые могут произойти в государственном органе (организации).

Перечень аттестованных центров кибербезопасности в РБ

Наименование юридического лица	Дата и номер приказа	Срок действия
1. Республиканское унитарное предприятие «Национальный центр обмена трафиком» https://www.ncot.by/ru/	от 11.11.2023 №204	до 11.11.2026
2. Общество с ограниченной ответственностью «Надежные программы» https://hoster.by/	от 05.01.2024 №1	до 05.01.2027

Национальная команда реагирования на киберинциденты CERT.BY

- **Зона ответственности CERT.BY** — национальный сегмент сети Интернет.

- **Основная задача национальной команды реагирования на киберинциденты** – снижение уровня угроз информационной безопасности национального сегмента сети Интернет.

- **CERT.BY** осуществляет сбор, хранение и обработку статистических данных, связанных с распространением вредоносных программ и сетевых атак на территории Республики Беларусь, а также реагирование на сами инциденты как в информационных системах государственных органов и организаций, так и у самостоятельно обратившихся субъектов национального сегмента сети Интернет.

Виды угроз и инцидентов, на которые реагирует CERT.BY

Блокирование доступа к информации

Распространение вредоносного программного обеспечения

Несанкционированный доступ, модификация, похищение информации

Сетевые атаки

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь 25.07.2023 № 130 О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40

Национальный правовой Интернет-портал Республики Беларусь, 28.07.2023, 7/5425

ПРИКАЗ ОПЕРАТИВНО-АНАЛИТИЧЕСКОГО ЦЕНТРА ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ
25 июля 2023 г. № 130

О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40

На основании пункта 3 Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности» ПРИКАЗЫВАЮ:

1. Утвердить:

Положение о порядке информационного взаимодействия элементов национальной системы обеспечения кибербезопасности (прилагается);

Положение о порядке функционирования национальной команды реагирования на киберинциденты Национального центра обеспечения кибербезопасности и реагирования на киберинциденты, команд реагирования на киберинциденты центров обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций (прилагается);

Положение о порядке проведения аттестации центров обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций (прилагается).

2. Установить состав технических параметров киберинцидента согласно приложению 1.

3. Определить:

требования к центрам обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций согласно приложению 2;

типовую структуру центров обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций согласно приложению 3;

требования по кибербезопасности объектов информационной инфраструктуры государственных органов и иных организаций согласно приложению 4.

4. Настоящий приказ вступает в силу с 17 августа 2023 г.

Начальник **А.Ю.Павлюченко**

- **В указе приводятся:**
- **СОСТАВ** технических параметров киберинцидента
- **ТРЕБОВАНИЯ** к центрам обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций
- **ТИПОВАЯ СТРУКТУРА** центров обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций
- **ТРЕБОВАНИЯ** по кибербезопасности объектов информационной инфраструктуры государственных органов и иных организаций
- **ПОЛОЖЕНИЕ** о порядке информационного взаимодействия элементов национальной системы обеспечения кибербезопасности
- **ПЕРЕЧЕНЬ** типов и записей событий информационной безопасности
- **ПОЛОЖЕНИЕ** о порядке функционирования национальной команды реагирования на киберинциденты Национального центра обеспечения кибербезопасности и реагирования на киберинциденты, команд реагирования на киберинциденты центров обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций
- **ПОЛОЖЕНИЕ** о порядке проведения аттестации центров обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций
- **ЗАЯВЛЕНИЕ** о проведении аттестации центра кибербезопасности
- https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2023%20-%20130.pdf

СОСТАВ технических параметров киберинцидента

Приложение 1
к приказу
Оперативно-аналитического
центра при Президенте
Республики Беларусь
25.07.2023 № 130

СОСТАВ
технических параметров киберинцидента

1. Технические параметры киберинцидента включают следующую информацию:
уровень киберинцидента и его наименование;
сетевые (IP) адреса версий 4 и (или) 6, подсети адресов объектов информационной инфраструктуры (при наличии);
доменные имена, связанные с объектами информационной инфраструктуры (при наличии);
уникальный идентификатор киберинцидента;
адреса электронной почты, URI-адреса объектов информационной инфраструктуры (при наличии);
сетевые (IP) адреса версий 4 и (или) 6, подсети адресов источников киберинцидента (при наличии);
доменные имена, связанные с источниками киберинцидента (при наличии);
адреса электронной почты, URI-адреса, связанные с источниками киберинцидента (при наличии);
вредоносные программы (при наличии);
идентификатор уязвимости с указанием системы классификации уязвимостей* (при наличии);
типы операционных систем, установленных на объектах информационной инфраструктуры;
дополнительные сведения, связанные с киберинцидентом (при наличии).
2. К киберинцидентам высокого уровня относятся:
внедрение и функционирование вредоносных программ на объектах информационной инфраструктуры;
несанкционированный доступ к объектам информационной инфраструктуры с использованием информационно-коммуникационных технологий;
использование объектов информационной инфраструктуры для осуществления кибератак и (или) распространения вредоносных программ;
прослушивание, захват, перенаправление сетевого трафика объектов информационной инфраструктуры;
рассылка незапрашиваемой информации (спама) с объектов информационной

- В документе **приводятся**:
  - **Технические параметры киберинцидента**
  - **Параметры киберинцидентам высокого и низкого уровня относятся**

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь 25.07.2023 № 130
О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40
https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2023%20-%20130.pdf

СОСТАВ технических параметров киберинцидента

- **1. Технические параметры киберинцидента включают следующую информацию:**
- уровень киберинцидента и его наименование;
- сетевые (IP) адреса версий 4 и (или) 6, подсети адресов объектов информационной инфраструктуры (при наличии);
- доменные имена, связанные с объектами информационной инфраструктуры (при наличии);
- уникальный идентификатор киберинцидента;
- адреса электронной почты, URI-адреса объектов информационной инфраструктуры (при наличии);
- сетевые (IP) адреса версий 4 и (или) 6, подсети адресов источников киберинцидента (при наличии);
- доменные имена, связанные с источниками киберинцидента (при наличии);
- адреса электронной почты, URI-адреса, связанные с источниками киберинцидента (при наличии);
- вредоносные программы (при наличии);
- идентификатор уязвимости с указанием системы классификации уязвимостей* (при наличии);
- типы операционных систем, установленных на объектах информационной инфраструктуры;
- дополнительные сведения, связанные с киберинцидентом (при наличии).

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь 25.07.2023 № 130
О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40
https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2023%20-%20130.pdf

СОСТАВ технических параметров киберинцидента

- **2. К киберинцидентам ВЫСОКОГО УРОВНЯ относятся:**
- внедрение и функционирование вредоносных программ на объектах информационной инфраструктуры;
- несанкционированный доступ к объектам информационной инфраструктуры с использованием информационно-коммуникационных технологий;
- использование объектов информационной инфраструктуры для осуществления кибератак и (или) распространения вредоносных программ;
- прослушивание, захват, перенаправление сетевого трафика объектов информационной инфраструктуры;
- рассылка незапрашиваемой информации (спама) с объектов информационной инфраструктуры;
- эксплуатация уязвимостей на объектах информационной инфраструктуры;
- прекращение функционирования объектов информационной инфраструктуры, вызванное кибератакой типа «отказ в обслуживании».

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь 25.07.2023 № 130
О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40
https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2023%20-%20130.pdf

СОСТАВ технических параметров киберинцидента

- **3. К киберинцидентам НИЗКОГО УРОВНЯ относятся:**
- попытка внедрения вредоносных программ на объектах информационной инфраструктуры;
- проведение кибератаки типа «отказ в обслуживании», направленной на объекты информационной инфраструктуры, не вызвавшей негативных последствий;
- попытка эксплуатации уязвимостей на объектах информационной инфраструктуры;
- сканирование объектов информационной инфраструктуры в целях поиска уязвимостей;
- попытка несанкционированного доступа к объектам информационной инфраструктуры;
- прекращение функционирования объектов информационной инфраструктуры, не связанное с киберинцидентом высокого уровня;
- попытка использования объектов информационной инфраструктуры для распространения вредоносных программ;
- попытка проведения кибератаки на веб-приложения и иные сетевые протоколы и службы;
- использование вычислительных мощностей объектов информационной инфраструктуры для проведения кибератак.

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь 25.07.2023 № 130
О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40
https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2023%20-%20130.pdf

ПЕРЕЧЕНЬ типов и записей событий ИБ

- **1. Для операционных систем:**
- запуск и (или) остановка системы;
- запуск и (или) остановка процессов;
- подключение съемных машинных носителей информации;
- подключение иных периферийных устройств к портам ввода (вывода) (мобильные устройства, сетевые адаптеры, беспроводные модемы и иные);
- установка и удаление программного обеспечения (изменение компонентов программного обеспечения);
- аутентификация (вход и (или) выход) пользователей в операционной системе, успешные и неуспешные попытки аутентификации;
- использование привилегированных учетных записей пользователей;
- создание, удаление, модификация учетных записей пользователей;

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь 25.07.2023 № 130
О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40
https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2023%20-%20130.pdf

ПЕРЕЧЕНЬ типов и записей событий ИБ

- **1. Для операционных систем:**
- неудавшиеся или отмененные действия пользователя и (или) процессы;
- создание или изменение параметров заданий в планировщике задач;
- установка, удаление, перезапуск, ошибка запуска службы и (или) сервиса;
- изменение системной конфигурации, в том числе сетевых настроек и средств межсетевого экранирования;
- изменение или попытки изменения настроек и средств управления защитой системы, в том числе антивирусного программного обеспечения, систем обнаружения и предотвращения вторжений;
- контроль несанкционированных сетевых соединений, в том числе попыток несанкционированного удаленного доступа, создания общих сетевых ресурсов, использования нестандартных сетевых портов.

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь 25.07.2023 № 130
О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40
https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2023%20-%20130.pdf

ПЕРЕЧЕНЬ типов и записей событий ИБ

- **2. Для систем управления базами данных:**
- контроль сессий (успешные и (или) неуспешные авторизация, регистрация пользователей, попытки использования незарегистрированных учетных записей);
- все действия пользователей, имеющих административные привилегии (включая команды «select», «create», «alter», «drop», «truncate», «rename», «insert», «update», «delete», «call (execute)», «lock»);
- все действия пользователей, имеющих права на присвоение привилегий другим пользователям («grant», «revoke», «deny»).

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь 25.07.2023 № 130
О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40
https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2023%20-%20130.pdf

ПЕРЕЧЕНЬ типов и записей событий ИБ

- **3. Для телекоммуникационного оборудования:**
- запуск и (или) остановка системы;
- изменение системной конфигурации;
- создание, удаление, модификация локальных учетных записей пользователей;
- использование привилегированных учетных записей пользователей;
- подключение и (или) отключение устройства ввода (вывода);
- неудавшиеся или отмененные действия пользователей;
- включение, отключение, перезапуск сетевых интерфейсов.

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь 25.07.2023 № 130
О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40
https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2023%20-%20130.pdf

ПЕРЕЧЕНЬ типов и записей событий ИБ

- **4. Для прикладного программного обеспечения:**
- аутентификация (вход и (или) выход) пользователей, успешные и неуспешные попытки аутентификации;
- создание, копирование, перемещение, удаление, модификация учетных записей пользователей и конфигурационных файлов;
- неудавшиеся или отмененные действия пользователей;
- действия пользователей (доступ к объекту (данным), изменения объекта (данных), удаление объекта (данных).

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь 25.07.2023 № 130
О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40
https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2023%20-%20130.pdf

ПЕРЕЧЕНЬ типов и записей событий ИБ

- **5. Для средств защиты информации:**
- создание, копирование, перемещение, удаление, модификация учетных записей пользователей и конфигурационных файлов;
- запуск и (или) остановка службы;
- изменение системной конфигурации;
- создание, удаление, модификация учетных записей пользователей.

Закон «О государственных секретах»

Закон Республики Беларусь от 19 июля 2010 г. N 170-З «О государственных секретах» http://kgb.by/ru/zakon170-3/

Закон «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.

- **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.

Закон Республики Беларусь от 19 июля 2010 г. N 170-З «О государственных секретах» http://kgb.by/ru/zakon170-3/

Закон «О государственных секретах»

- **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;
- **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.

Закон Республики Беларусь от 19 июля 2010 г. N 170-З «О государственных секретах» http://kgb.by/ru/zakon170-3/

Закон «О государственных секретах»

- **Гриф секретности** - реквизит, проставляемый на носителе государственных секретов и (или) сопроводительной документации к нему, свидетельствующий о степени секретности содержащихся на этом носителе государственных секретов;
- **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".

Закон Республики Беларусь от 19 июля 2010 г. N 170-З «О государственных секретах» http://kgb.by/ru/zakon170-3/

Закон «О государственных секретах»

- **Степень секретности** - показатель важности государственных секретов, определяющий меры и средства защиты государственных секретов;

- **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**".

Закон Республики Беларусь от 19 июля 2010 г. N 170-З «О государственных секретах» http://kgb.by/ru/zakon170-3/

Закон «О государственных секретах»

- **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;

Закон Республики Беларусь от 19 июля 2010 г. N 170-З «О государственных секретах» http://kgb.by/ru/zakon170-3/

Закон «О государственных секретах»

- **Допуск к государственным секретам** регулируется
  - **Статьей 34.** Допуск к государственным секретам граждан и
  - **Статьей 35.** Допуск к государственным секретам граждан Республики Беларусь в связи с их избранием (назначением) на должность

- **Формы допуска к государственным секретам**
- В зависимости от степени секретности устанавливаются три формы допуска к государственным секретам:
  - **форма N 1** - форма допуска к государственной тайне, имеющей степень секретности "Особой важности";
  - **форма N 2** - форма допуска к государственной тайне, имеющей степень секретности "Совершенно секретно";
  - **форма N 3** - форма допуска к служебной тайне, имеющей степень секретности "Секретно".

Закон Республики Беларусь от 19 июля 2010 г. N 170-З «О государственных секретах» http://kgb.by/ru/zakon170-3/

Закон «О государственных секретах»

- **Техническая защита государственных секретов** - деятельность, направленная на обеспечение защиты государственных секретов техническими мерами, за исключением технических мер защиты государственных секретов, применяемых в системах шифрованной, других видов специальной связи и при использовании криптографических средств защиты государственных секретов.
- **Средства защиты государственных секретов** - технические, программные, криптографические и другие средства, используемые для защиты государственных секретов, а также средства контроля эффективности защиты государственных секретов;

Закон Республики Беларусь от 19 июля 2010 г. N 170-З «О государственных секретах» http://kgb.by/ru/zakon170-3/

Постановление Совета Министров Республики Беларусь от 12 августа 2014 г. № 783 "О служебной информации ограниченного распространения и информации, составляющей коммерческую тайну"

ПОСТАНОВЛЕНИЕ СОВЕТА МИНИСТРОВ РЕСПУБЛИКИ БЕЛАРУСЬ
12 августа 2014 г. № 783

О служебной информации ограниченного распространения и информации, составляющей коммерческую тайну

Изменения и дополнения:

Постановление Совета Министров Республики Беларусь от 18 марта 2015 г. № 211 (Национальный правовой Интернет-портал Республики Беларусь, 21.03.2015, 5/40283) <C21500211>;

Постановление Совета Министров Республики Беларусь от 20 октября 2015 г. № 873 (Национальный правовой Интернет-портал Республики Беларусь, 23.10.2015, 5/41180) <C21500873>;

Постановление Совета Министров Республики Беларусь от 13 февраля 2018 г. № 124 (Национальный правовой Интернет-портал Республики Беларусь, 15.02.2018, 5/44822) <C21800124>;

Постановление Совета Министров Республики Беларусь от 13 ноября 2018 г. № 815 (Национальный правовой Интернет-портал Республики Беларусь, 15.11.2018, 5/45804) <C21800815>;

Постановление Совета Министров Республики Беларусь от 12 марта 2020 г. № 145 (Национальный правовой Интернет-портал Республики Беларусь, 14.03.2020, 5/47891) <C22000145>;

Постановление Совета Министров Республики Беларусь от 14 сентября 2020 г. № 533 (Национальный правовой Интернет-портал Республики Беларусь, 17.09.2020, 5/48362) <C22000533>;

Постановление Совета Министров Республики Беларусь от 10 апреля 2023 г. № 237 (Национальный правовой Интернет-портал Республики Беларусь, 13.04.2023, 5/51553) <C22300237>

(Извлечение)

Во исполнение абзаца четвертого статьи 23 Закона Республики Беларусь от 5 января 2013 г. № 16-З «О коммерческой тайне» и абзаца второго части первой статьи 2 Закона Республики Беларусь от 4 января 2014 г. № 102-З «О внесении изменений и дополнений в Закон Республики Беларусь «Об информации, информатизации и защите информации» Совет Министров Республики Беларусь ПОСТАНОВЛЯЕТ:

1. Утвердить Положение о порядке проставления ограничительного грифа «Для служебного пользования», грифа «Коммерческая тайна» и ведения делопроизводства по документам, содержащим служебную информацию ограниченного распространения и информацию, составляющую коммерческую тайну (прилагается).

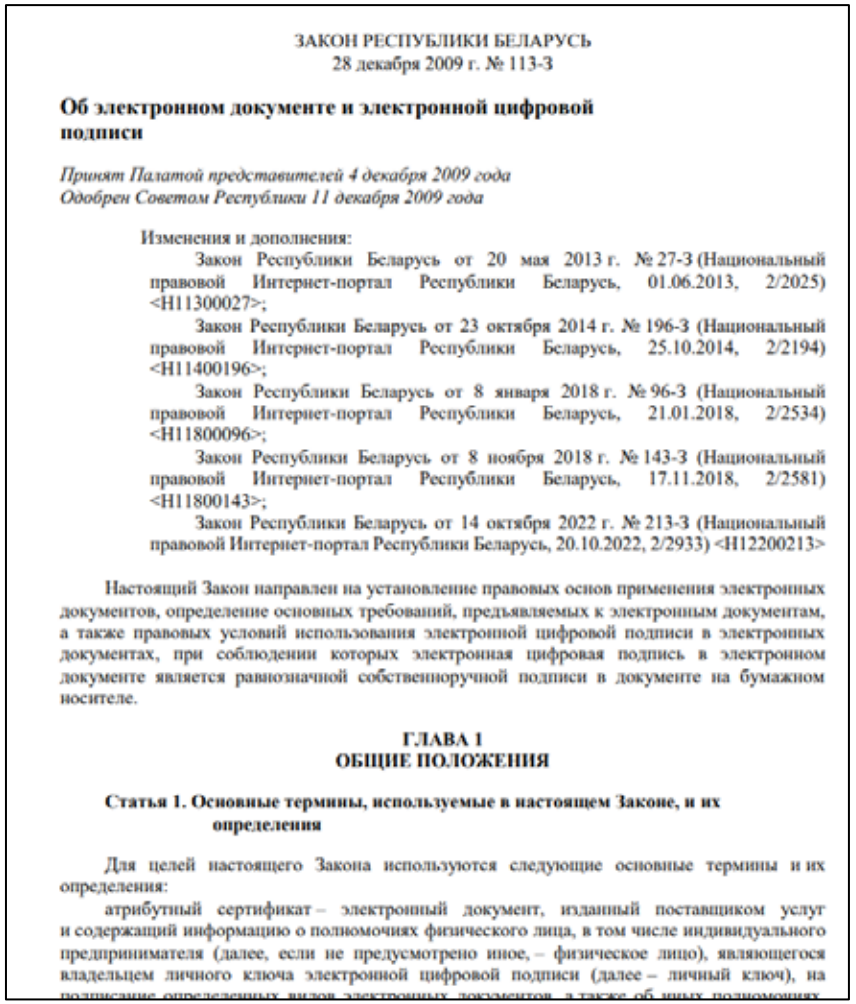
2. Определить перечень сведений, относящихся к служебной информации ограниченного распространения, согласно приложению.

3. Государственным органам, государственным организациям, иным юридическим

- **В настоящем Положении** в соответствии с частями второй и четвертой статьи 181 Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» и абзацем четвертым статьи 23 Закона Республики Беларусь «О коммерческой тайне» **определяются:**
- **порядок проставления на документах ограничительного грифа «Для служебного пользования»** и ведения делопроизводства в государственных органах и государственных организациях (далее, если не указано иное, – государственные органы), иных юридических лицах, организациях, не являющихся юридическими лицами (далее – юридические лица), – по документам, содержащим служебную информацию ограниченного распространения;
- **порядок проставления на документах грифа «Коммерческая тайна»** и ведения делопроизводства в государственных органах, получивших в соответствии с законодательством доступ к информации, составляющей коммерческую тайну (далее – государственные органы, получившие доступ к коммерческой тайне), – по документам, содержащим информацию, составляющую коммерческую тайну.

https://www.oac.gov.by/public/content/files/files/law/resolutions-sm/2014-783.pdf

Закон Республики Беларусь от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи»



ЗАКОН РЕСПУБЛИКИ БЕЛАРУСЬ
28 декабря 2009 г. № 113-З

Об электронном документе и электронной цифровой подписи

Принят Палатой представителей 4 декабря 2009 года
Одобрен Советом Республики 11 декабря 2009 года

Изменения и дополнения:

Закон Республики Беларусь от 20 мая 2013 г. № 27-З (Национальный правовой Интернет-портал Республики Беларусь, 01.06.2013, 2/2025) <H11300027>;

Закон Республики Беларусь от 23 октября 2014 г. № 196-З (Национальный правовой Интернет-портал Республики Беларусь, 25.10.2014, 2/2194) <H11400196>;

Закон Республики Беларусь от 8 января 2018 г. № 96-З (Национальный правовой Интернет-портал Республики Беларусь, 21.01.2018, 2/2534) <H11800096>;

Закон Республики Беларусь от 8 ноября 2018 г. № 143-З (Национальный правовой Интернет-портал Республики Беларусь, 17.11.2018, 2/2581) <H11800143>;

Закон Республики Беларусь от 14 октября 2022 г. № 213-З (Национальный правовой Интернет-портал Республики Беларусь, 20.10.2022, 2/2933) <H12200213>

Настоящий Закон направлен на установление правовых основ применения электронных документов, определение основных требований, предъявляемых к электронным документам, а также правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе является равнозначной собственноручной подписи в документе на бумажном носителе.

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

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

Для целей настоящего Закона используются следующие основные термины и их определения:

атрибутный сертификат – электронный документ, изданный поставщиком услуг и содержащий информацию о полномочиях физического лица, в том числе индивидуального предпринимателя (далее, если не предусмотрено иное, – физическое лицо), являющегося владельцем личного ключа электронной цифровой подписи (далее – личный ключ), на

- Настоящий Закон направлен на установление правовых основ применения электронных документов, определение основных требований, предъявляемых к электронным документам, а также правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе является равнозначной собственноручной подписи в документе на бумажном носителе.
- https://www.oac.gov.by/public/content/files/files/law/laws-rb/113-z.pdf

ОПЕРАТИВНО-АНАЛИТИЧЕСКИЙ ЦЕНТР ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ

https://www.oac.gov.by

Информация об ОАЦ

Право

Новости

Деятельность ОАЦ в сфере кибербезопасности и защиты информации

Безопасный Интернет

Лотерейная деятельность и электронные интерактивные игры

Борьба с мошенничеством на сетях электросвязи

Обращения граждан и юридических лиц

Оперативно-аналитический центр при Президенте Республики Беларусь

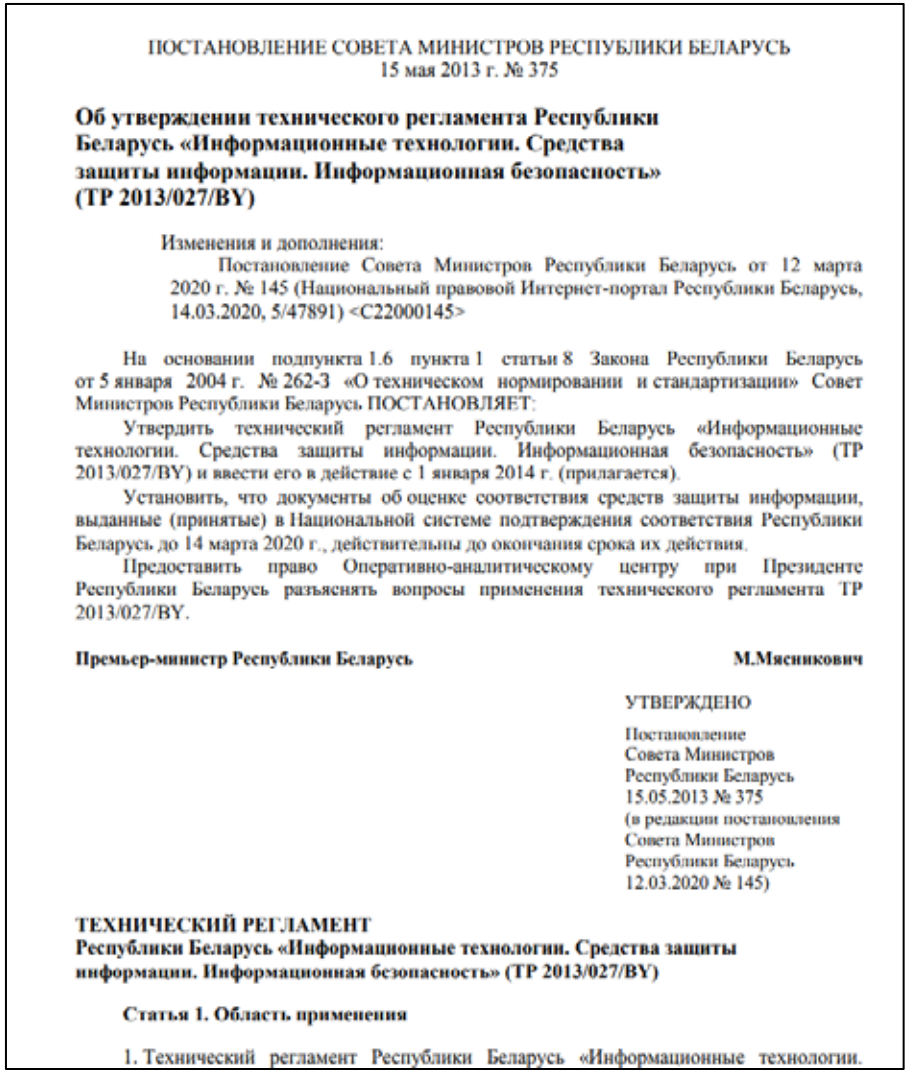
- **Оперативно-аналитический центр** при Президенте Республики Беларусь (ОАЦ) является государственным органом, **осуществляющим регулирование деятельности по обеспечению защиты информации**, **содержащей сведения, составляющие государственные секреты** Республики Беларусь или иные сведения, охраняемые в соответствии с законодательством, от утечки по техническим каналам, несанкционированных и непреднамеренных воздействий.

- https://oac.gov.by/ - Официальный сайт ОАЦ

Оперативно-аналитический центр при Президенте Республики Беларусь

- **Право**
- Законы Республики Беларусь
  https://oac.gov.by/law/laws-of-the-republic-of-belarus
- Указы Президента Республики Беларусь
  https://oac.gov.by/law/decrees-of-the-president-of-the-republic-of-belarus
- Постановления Совета Министров Республики Беларусь
  https://oac.gov.by/law/resolutions-of-the-council-of-ministers-of-the-republic-of-belarus
- Постановления Оперативно-аналитического центра при Президенте Республики Беларусь
  https://oac.gov.by/law/resolutions-of-the-oac
- Приказы Оперативно-аналитического центра при Президенте Республики Беларусь
  https://oac.gov.by/law/orders-of-the-oac

ТР 2013/027/BY «Информационные технологии. Средства защиты информации. Информационная безопасность»



ПОСТАНОВЛЕНИЕ СОВЕТА МИНИСТРОВ РЕСПУБЛИКИ БЕЛАРУСЬ
15 мая 2013 г. № 375

Об утверждении технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY)

Изменения и дополнения:
Постановление Совета Министров Республики Беларусь от 12 марта 2020 г. № 145 (Национальный правовой Интернет-портал Республики Беларусь, 14.03.2020, 5/47891) <C22000145>

На основании подпункта 1.6 пункта 1 статьи 8 Закона Республики Беларусь от 5 января 2004 г. № 262-З «О техническом нормировании и стандартизации» Совет Министров Республики Беларусь ПОСТАНОВЛЯЕТ:

Утвердить технический регламент Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) и ввести его в действие с 1 января 2014 г. (прилагается).

Установить, что документы об оценке соответствия средств защиты информации, выданные (принятые) в Национальной системе подтверждения соответствия Республики Беларусь до 14 марта 2020 г., действительны до окончания срока их действия.

Предоставить право Оперативно-аналитическому центру при Президенте Республики Беларусь разъяснять вопросы применения технического регламента ТР 2013/027/BY.

Премьер-министр Республики Беларусь **М.Мясникович**

УТВЕРЖДЕНО
Постановление
Совета Министров
Республики Беларусь
15.05.2013 № 375
(в редакции постановления
Совета Министров
Республики Беларусь
12.03.2020 № 145)

ТЕХНИЧЕСКИЙ РЕГЛАМЕНТ
Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY)

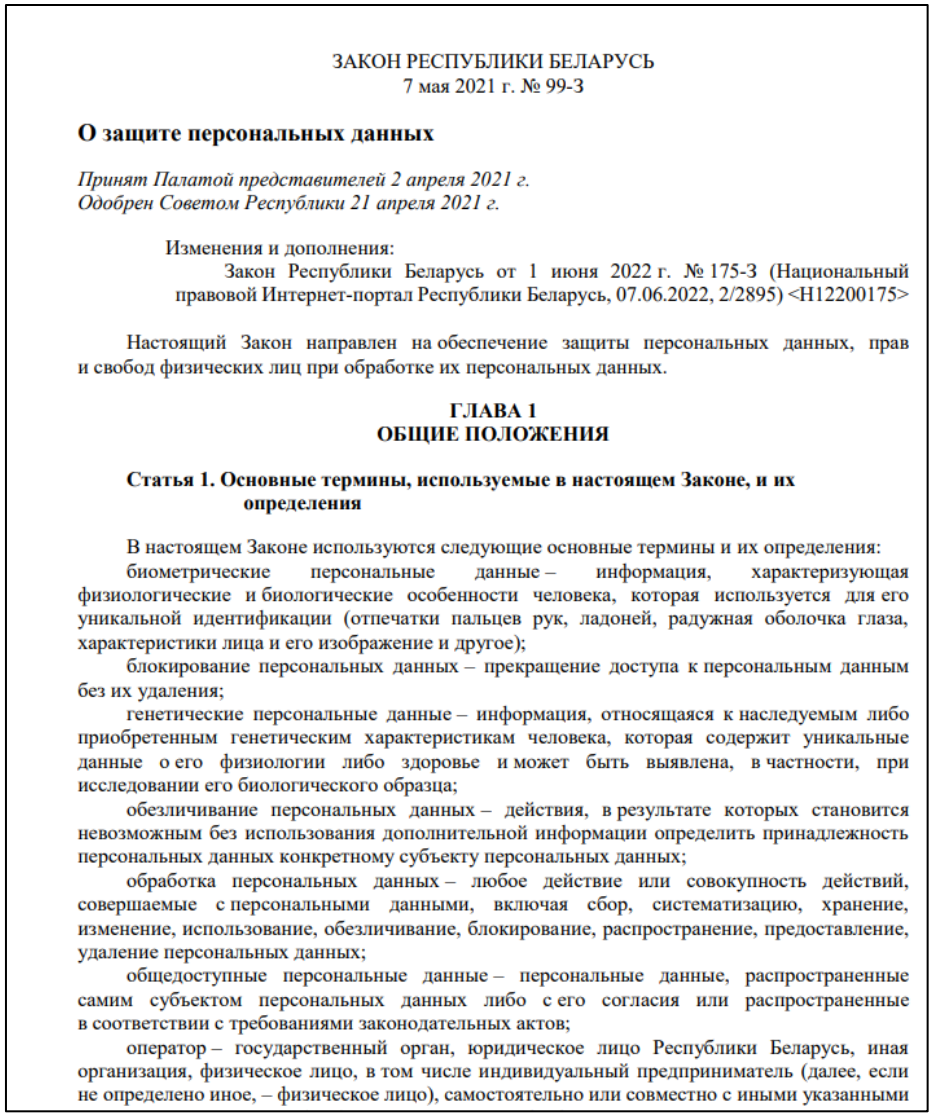
Статья 1. Область применения

1. Технический регламент Республики Беларусь «Информационные технологии.

- 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

ТР 2013/027/BY «Информационные технологии. Средства защиты информации. Информационная безопасность»
http://www.government.by/upload/docs/file0bcd50754d1e60d7.PDF

Закон РБ от 7 мая 2021 г. № 99-З «О защите персональных данных»



ЗАКОН РЕСПУБЛИКИ БЕЛАРУСЬ
7 мая 2021 г. № 99-З

О защите персональных данных

Принят Палатой представителей 2 апреля 2021 г.
Одобрен Советом Республики 21 апреля 2021 г.

Изменения и дополнения:
Закон Республики Беларусь от 1 июня 2022 г. № 175-З (Национальный правовой Интернет-портал Республики Беларусь, 07.06.2022, 2/2895) <H12200175>

Настоящий Закон направлен на обеспечение защиты персональных данных, прав и свобод физических лиц при обработке их персональных данных.

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:
биометрические персональные данные – информация, характеризующая физиологические и биологические особенности человека, которая используется для его уникальной идентификации (отпечатки пальцев рук, ладоней, радужная оболочка глаза, характеристики лица и его изображение и другое);
блокирование персональных данных – прекращение доступа к персональным данным без их удаления;
генетические персональные данные – информация, относящаяся к наследуемым либо приобретенным генетическим характеристикам человека, которая содержит уникальные данные о его физиологии либо здоровье и может быть выявлена, в частности, при исследовании его биологического образца;
обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
обработка персональных данных – любое действие или совокупность действий, совершаемые с персональными данными, включая сбор, систематизацию, хранение, изменение, использование, обезличивание, блокирование, распространение, предоставление, удаление персональных данных;
общедоступные персональные данные – персональные данные, распространенные самим субъектом персональных данных либо с его согласия или распространенные в соответствии с требованиями законодательных актов;
оператор – государственный орган, юридическое лицо Республики Беларусь, иная организация, физическое лицо, в том числе индивидуальный предприниматель (далее, если не определено иное, – физическое лицо), самостоятельно или совместно с иными указанными

- Настоящий Закон **направлен на обеспечение защиты персональных данных**, прав и свобод физических лиц при обработке их персональных данных.

- ***Подробно будет рассмотрен в лекции на тему «Защита персональных данных».***

Закон РБ от 7 мая 2021 г. № 99-З «О защите персональных данных»
https://pravo.by/upload/docs/op/H12100099_1620939600.pdf

Стандарты Республики Беларусь «Информационные технологии и безопасность»

Обозначение / технологический номер	Наименование	Дата введения	Состояние
СТБ 34.101.1-2014 (ISO/IEC 15408-1:2009)	Информационные технологии и безопасность. **Критерии оценки безопасности информационных технологий**. Часть 1. Введение и общая модель	01.09.2014	Взамен
СТБ 34.101.2-2014 (ISO/IEC 15408-2:2008)	Информационные технологии и безопасность. **Критерии оценки безопасности информационных технологий**. Часть 2. Функциональные требования безопасности	01.09.2014	Взамен
СТБ 34.101.3-2014 (ISO/IEC 15408-3:2008)	Информационные технологии и безопасность. **Критерии оценки безопасности информационных технологий**. Часть 3. Гарантийные требования безопасности	01.09.2014	Взамен
СТБ 34.101.8-2006	Информационные технологии. Методы и средства безопасности. **Программные и программно-аппаратные средства защиты от воздействия вредоносных программ и антивирусные программные средства**. Общие требования	01.07.2006	Взамен
СТБ 34.101.9-2004	Информационные технологии. **Требования к защите информации от несанкционированного доступа, устанавливаемые в техническом задании на создание автоматизированной системы**	01.09.2004	Введен впервые

Стандарты Республики Беларусь «Информационные технологии и безопасность»

Обозначение / технологический номер	Наименование	Дата введения	Состояние
СТБ 34.101.10-2004	Информационные технологии. **Средства защиты информации от несанкционированного доступа в автоматизированных системах.** Общие требования	01.09.2004	Введен впервые
СТБ 34.101.11-2009	Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. **Профиль защиты операционной системы сервера для использования в доверенной зоне корпоративной сети**	01.09.2009	Взамен
СТБ 34.101.12-2007	Информационные технологии. Методы и средства безопасности. **Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Оценка качества**	01.10.2007	Взамен
СТБ 34.101.13-2009	Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. **Профиль защиты операционной системы сервера для использования в демилитаризованной зоне корпоративной сети**	01.09.2009	Взамен
СТБ 34.101.14-2017	Информационные технологии. Методы и средства безопасности. **Программные средства маршрутизатора.** Общие требования	01.04.2018	Взамен

Стандарты Республики Беларусь «Информационные технологии и безопасность»

Обозначение / технологический номер	Наименование	Дата введения	Состояние
СТБ 34.101.15-2007	Информационные технологии. Методы и средства безопасности. **Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Типовая программа и методика испытаний**	01.11.2007	Взамен
СТБ 34.101.16-2009	Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. **Профиль защиты программных средств коммутатора для использования в доверенной зоне корпоративной сети**	01.08.2009	Взамен
СТБ 34.101.17-2012	Информационные технологии и безопасность. **Синтаксис запроса на получение сертификата**	01.08.2012	Взамен
СТБ 34.101.18-2009	Информационные технологии. **Синтаксис обмена персональной информацией**	01.09.2009	Взамен
СТБ 34.101.19-2012	Информационные технологии и безопасность. **Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей**	01.08.2012	Взамен
СТБ 34.101.20-2009	Информационные технологии. **Синтаксис криптографической информации для токенов**	01.09.2009	Взамен

Стандарты Республики Беларусь «Информационные технологии и безопасность»

Обозначение / технологический номер	Наименование	Дата введения	Состояние
СТБ 34.101.21-2009	Информационные технологии. **Интерфейс обмена информацией с аппаратно-программным носителем криптографической информации (токеном)**	01.09.2009	Взамен
СТБ 34.101.22-2009	Информационные технологии. **Криптография на основе алгоритма RSA**	01.09.2009	Взамен
СТБ 34.101.23-2012	Информационные технологии и безопасность. **Синтаксис криптографических сообщений**	01.08.2012	Введен впервые
СТБ 34.101.26-2012	Информационные технологии и безопасность. **Онлайновый протокол проверки статуса сертификата (OCSP)**	01.08.2012	Введен впервые
СТБ 34.101.27-2022	Информационные технологии и безопасность. **Средства криптографической защиты информации.** Требования безопасности	01.01.2023	Взамен
СТБ 34.101.30-2017	Информационные технологии. Методы и средства безопасности. **Информационные системы. Классификация**	01.10.2017	Взамен
СТБ 34.101.31-2020	Информационные технологии и безопасность. **Алгоритмы шифрования и контроля целостности**	01.09.2021	Взамен

Стандарты Республики Беларусь «Информационные технологии и безопасность»

Обозначение / технологический номер	Наименование	Дата введения	Состояние
СТБ 34.101.35-2011	Информационные технологии. Методы и средства безопасности. Объекты информатизации. **Профиль защиты класса Б3**	01.03.2012	Взамен
СТБ 34.101.36-2011	Информационные технологии. Методы и средства безопасности. Объекты информатизации. **Профиль защиты класса А2**	01.03.2012	Взамен
СТБ 34.101.37-2017	Информационные технологии и безопасность. **Методы и средства безопасности. Системы управления сайта.** Общие требования	01.04.2018	Взамен
СТБ 34.101.41-2013	Информационные технологии и безопасность. **Обеспечение информационной безопасности банков Республики Беларусь.** Общие положения	01.07.2014	Введен впервые
СТБ 34.101.42-2013	Информационные технологии и безопасность. **Обеспечение информационной безопасности банков Республики Беларусь. Аудит информационной безопасности**	01.07.2014	Введен впервые
СТБ 34.101.45-2013	Информационные технологии и безопасность. **Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых**	01.01.2014	Взамен

Стандарты Республики Беларусь «Информационные технологии и безопасность»

Обозначение / технологический номер	Наименование	Дата введения	Состояние
СТБ 34.101.47-2017	Информационные технологии и безопасность. **Криптографические алгоритмы генерации псевдослучайных чисел**	01.09.2017	Взамен
СТБ 34.101.48-2012	Информационные технологии и безопасность. **Требования к политике применения сертификатов удостоверяющих центров**	01.08.2012	Введен впервые
СТБ 34.101.49-2012	Информационные технологии и безопасность. **Формат карточки открытого ключа**	01.08.2012	Введен впервые
СТБ 34.101.50-2019	Информационные технологии и безопасность. **Правила регистрации объектов информационных технологий**	01.10.2019	Взамен
СТБ 34.101.52-2016	Информационные технологии. Методы и средства безопасности. **Критически важные объекты информатизации. Классификация**	01.04.2017	Взамен
СТБ 34.101.53-2016	Информационные технологии. Методы и средства безопасности. **Профиль защиты критически важных объектов информатизации класса А1-у**	01.04.2017	Взамен

Стандарты Республики Беларусь «Информационные технологии и безопасность»

Обозначение / технологический номер	Наименование	Дата введения	Состояние
СТБ 34.101.54-2016	Информационные технологии. Методы и средства безопасности. **Профиль защиты критически важных объектов информатизации класса А2-у**	01.04.2017	Взамен
СТБ 34.101.55-2016	Информационные технологии. Методы и средства безопасности. **Профиль защиты критически важных объектов информатизации класса Б1-у**	01.04.2017	Взамен
СТБ 34.101.56-2016	Информационные технологии. Методы и средства безопасности. **Профиль защиты критически важных объектов информатизации класса Б2-у**	01.04.2017	Взамен
СТБ 34.101.57-2016	Информационные технологии. Методы и средства безопасности. **Профиль защиты критически важных объектов информатизации класса В1-у**	01.04.2017	Взамен
СТБ 34.101.58-2016	Информационные технологии. Методы и средства безопасности. **Профиль защиты критически важных объектов информатизации класса В2-у**	01.04.2017	Взамен
СТБ 34.101.59-2016	Информационные технологии и безопасность. **Задание по безопасности. Методические указания по разработке**	01.04.2017	Взамен

Стандарты Республики Беларусь «Информационные технологии и безопасность»

Обозначение / технологический номер	Наименование	Дата введения	Состояние
СТБ 34.101.60-2014	Информационные технологии и безопасность. **Алгоритмы разделения секрета**	01.09.2014	Взамен
СТБ 34.101.61-2013	Информационные технологии и безопасность. Обеспечение информационной безопасности **банков** Республики Беларусь. **Методика оценки рисков нарушения информационной безопасности**	01.07.2014	Введен впервые
СТБ 34.101.62-2013	Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. **Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТБ 34.101.41**	01.07.2014	Введен впервые
СТБ 34.101.65-2014	Информационные технологии и безопасность. **Протокол защиты транспортного уровня (TLS)**	01.09.2014	Введен впервые
СТБ 34.101.66-2014	Информационные технологии и безопасность. **Протоколы формирования общего ключа на основе эллиптических кривых**	01.09.2014	Введен впервые
СТБ 34.101.67-2014	Информационные технологии и безопасность. **Инфраструктура атрибутных сертификатов**	01.09.2014	Введен впервые

Стандарты Республики Беларусь «Информационные технологии и безопасность»

Обозначение / технологический номер	Наименование	Дата введения	Состояние
СТБ 34.101.68-2013	Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. **Методика оценки соответствия информационной безопасности банков Республики Беларусь требованиям СТБ 34.101.41**	01.07.2014	Введен впервые
СТБ 34.101.69-2014	Информационные технологии и безопасность. **Криптология.** Термины и определения	01.02.2015	Введен впервые
СТБ 34.101.70-2016	Информационные технологии. Методы и средства безопасности. **Методика оценки рисков информационной безопасности в информационных системах**	01.04.2017	Введен впервые
СТБ 34.101.72-2018	Информационные технологии. Методы и средства безопасности. **Технические средства обработки информации. Классификация угроз безопасности, связанных с наличием закладных устройств и недекларированных функций**	01.08.2018	Взамен
СТБ 34.101.73-2017	Информационные технологии. Методы и средства безопасности. **Межсетевые экраны.** Общие требования	01.01.2018	Введен впервые

Стандарты Республики Беларусь «Информационные технологии и безопасность»

Обозначение / технологический номер	Наименование	Дата введения	Состояние
СТБ 34.101.74-2017	Информационные технологии. **Системы сбора и обработки данных событий информационной безопасности.** Общие требования	01.10.2017	Введен впервые
СТБ 34.101.75-2017	Информационные технологии. **Системы обнаружения и предотвращения вторжений.** Общие требования	01.10.2017	Введен впервые
СТБ 34.101.76-2017	Информационные технологии. Методы и средства безопасности. **Системы обнаружения и предотвращения утечек информации из информационных систем.** Общие требования	01.04.2018	Введен впервые
СТБ 34.101.77-2020	Информационные технологии и безопасность. **Криптографические алгоритмы на основе sponge-функции**	01.09.2021	Взамен
СТБ 34.101.78-2019	Информационные технологии и безопасность. **Профиль инфраструктуры открытых ключей**	01.10.2019	Введен впервые
СТБ 34.101.79-2019	Информационные технологии и безопасность. **Криптографические токены**	01.10.2019	Введен впервые

Стандарты Республики Беларусь «Информационные технологии и безопасность»

Обозначение / технологический номер	Наименование	Дата введения	Состояние
СТБ 34.101.80-2019	Информационные технологии и безопасность. **Расширенные электронные цифровые подписи**	01.10.2019	Введен впервые
СТБ 34.101.81-2019	Информационные технологии и безопасность. **Протоколы службы заверения данных**	01.10.2019	Введен впервые
СТБ 34.101.82-2019	Информационные технологии и безопасность. **Протокол постановки штампа времени**	01.10.2019	Введен впервые
СТБ 34.101.87-2022	Информационные технологии и безопасность. **Инфраструктуры аутентификации**	01.07.2023	Введен впервые


КОДЕКС РЕСПУБЛИКИ БЕЛАРУСЬ
ОБ АДМИНИСТРАТИВНЫХ ПРАВОНАРУШЕНИЯХ
ПРОЦЕССУАЛЬНО-ИСПОЛНИТЕЛЬНЫЙ КОДЕКС
РЕСПУБЛИКИ БЕЛАРУСЬ
ОБ АДМИНИСТРАТИВНЫХ ПРАВОНАРУШЕНИЯХ
ГРАЖДАНСКИЙ ПРОЦЕССУАЛЬНЫЙ КОДЕКС
РЕСПУБЛИКИ БЕЛАРУСЬ
УГОЛОВНЫЙ КОДЕКС
РЕСПУБЛИКИ БЕЛАРУСЬ

Кодекс Республики Беларусь Об административных правонарушениях

- **Статья 10.5.** Отказ в предоставлении гражданину информации

- **ГЛАВА 23. Административные правонарушения в области связи и информации**
  - **Статья 23.4.** Несанкционированный доступ к компьютерной информации
  - **Статья 23.5.** Нарушение законодательства о средствах массовой информации
  - **Статья 23.6.** Разглашение коммерческой или иной охраняемой законом тайны
  - **Статья 23.7.** Нарушение законодательства о защите персональных данных
  - **Статья 23.8.** Разглашение служебной тайны по неосторожности
  - **Статья 23.9.** Нарушение требований по использованию национального сегмента сети Интернет
  - **Статья 23.10.** Нарушение правил оборота специальных технических средств, предназначенных для негласного получения информации

Кодекс Республики Беларусь Об административных правонарушениях
https://pravo.by/upload/docs/op/HK2100091_1611262800.pdf

Гражданский Кодекс Республики Беларусь

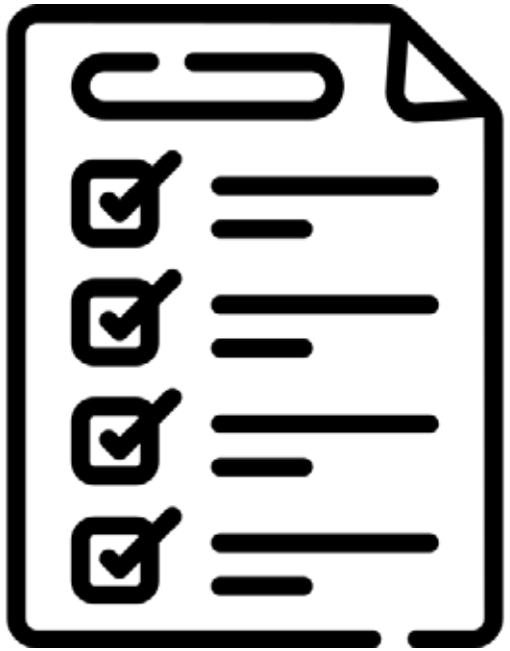
- **Статья 140.** Нераскрытая информация
  - 1. Информация (сведения о лицах, предметах, фактах, событиях, явлениях и процессах) охраняется в качестве нераскрытой информации, если она составляет служебную тайну или коммерческую тайну.
  - 2. В отношении информации может быть установлен режим коммерческой тайны при условии, что составляющие ее сведения не являются общеизвестными или легкодоступными третьим лицам в тех кругах, которые обычно имеют дело с подобного рода сведениями, имеют коммерческую ценность для их обладателя в силу неизвестности третьим лицам, не являются объектами исключительных прав на результаты интеллектуальной деятельности и не отнесены в установленном порядке к государственным секретам. Режим коммерческой тайны считается установленным после определения состава сведений, подлежащих охране в режиме коммерческой тайны, и принятия лицом, правомерно обладающим такими сведениями, совокупности мер, необходимых для обеспечения их конфиденциальности.
  - Сведения, в отношении которых не может быть установлен режим коммерческой тайны, определяются законодательными актами.
  - 3. Условия и порядок отнесения информации к служебной тайне определяются законодательством.
  - 4. Информация, составляющая служебную тайну или коммерческую тайну, защищается способами, предусмотренными законодательством.
  - **В случае незаконного ознакомления или незаконного использования, а также разглашения информации, которая составляет служебную тайну или коммерческую тайну, физические и юридические лица, государственные органы и их должностные лица обязаны возместить ее обладателю причиненные убытки**. Такая же обязанность возлагается на работников, разгласивших служебную тайну или коммерческую тайну вопреки обязательству о неразглашении коммерческой тайны, трудовому договору (контракту), и на контрагентов, сделавших это вопреки гражданско-правовому договору.

Гражданский Кодекс Республики Беларусь
https://pravo.by/document/?guid=3871&p0=hk9800218

Уголовный Кодекс Республики Беларусь

- **РАЗДЕЛ XII Преступления против компьютерной безопасности**
  - **Статья 349.** Несанкционированный доступ к компьютерной информации
  - **Статья 350.** Уничтожение, блокирование или модификация компьютерной информации
  - **Статья 352.** Неправомерное завладение компьютерной информацией
  - **Статья 354.** Разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств
  - **Статья 355.** Нарушение правил эксплуатации компьютерной системы или сети

Уголовный Кодекс Республики Беларусь
https://pravo.by/document/?guid=3871&p0=Hk9900275



Рекомендации Коллегии Евразийской экономической комиссии от 12 марта 2019 г. № 9

2.2 ПЕРЕЧЕНЬ стандартов и рекомендаций в области информационной безопасности, применяемых в рамках реализации цифровой повестки Евразийского экономического союза

https://pravo.by/document/?guid=3871&p0=F01900068

ПЕРЕЧЕНЬ стандартов и рекомендаций в области информационной безопасности, применяемых в рамках реализации цифровой повестки Евразийского экономического союза

- **I.** Разработка средств защиты информации и разработка приложений
- **II.** Создание и сопровождение систем управления информационной безопасностью
- **III.** Обеспечение сетевой безопасности и обеспечение защиты веб-сервисов
- **IV.** Обеспечение защиты информации с использованием средств криптографической защиты
- **V.** Обеспечение возможности использования электронной цифровой подписи (электронной подписи) и обеспечение функционирования сервисов доверенной третьей стороны

ПЕРЕЧЕНЬ стандартов и рекомендаций в области информационной безопасности, применяемых в рамках реализации цифровой повестки Евразийского экономического союза

- **VI.** Обеспечение доверия к цифровым сервисам
- **VII.** Обеспечение функций по идентификации субъектов электронного взаимодействия, в том числе сервисов информационно-коммуникационных технологий, и проверке правомочий

I. Разработка средств защиты информации и разработка приложений

- **1. ISO/IEC/IEEE 12207:2017** «Системная и программная инженерия. Процессы жизненного цикла программных средств» (Systems and software engineering – Software life cycle processes).
- **2. ГОСТ ИСО/МЭК 12207-2002** «Информационная технология. Процессы жизненного цикла программных средств».
- **3. СТ РК ISO/IEC 12207-2015** «Системная и программная инженерия. Процессы жизненного цикла программных средств».
- **4. ISO/IEC 27031:2011** «Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса» (Information technology – Security techniques – Guidelines for information and communications technology readiness for business continuity).
- **5. СТ РК ISO/IEC 27031-2013** «Информационные технологии. Методы обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий для обеспечения непрерывности бизнеса».
- **6. ISO/IEC 15408-1:2009** «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ.Часть 1. Введение и общая модель» (Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model).
- **7. СТ РК ISO/IEC 15408-1-2017** «Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».

I. Разработка средств защиты информации и разработка приложений

- **8. СТБ 34.101.1-2014 (15408-1:2009)** «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».
- **9. ISO/IEC 15408-2:2008** «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ.Часть 2. Функциональные требования безопасности» (Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components).
- **10. СТ РК ISO/IEC 15408-2-2017** «Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности».
- **11. СТБ 34.101.2-2014 (15408-2:2009)** «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности».
- **12. ISO/IEC 15408-3:2008** «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ.Часть 3. Требования к обеспечению защиты» (Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components).
- **13. СТ РК ISO/IEC 15408-3-2017** «Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования обеспечению защиты».
- **14. СТБ 34.101.3-2014 (15408-3:2009)** «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности».

II. Создание и сопровождение систем управления информационной безопасностью

- **15. СТБ ISO/IEC 27000-2012** «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Основные положения и словарь».
- **16. ISO/IEC 27001:2013** «Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (Information technology – Security techniques – Information security management systems – Requirements).
- **17. СТ РК ISO/IEC 27001-2015** «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования».
- **18. СТБ ISO/IEC 27001-2016** «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».
- **19. ISO/IEC 27002:2013** «Информационные технологии. Методы обеспечения безопасности. Свод правил по управлению защитой информации» (Information technology – Security techniques – Code of practice for information security controls).
- **20. СТ РК ISO/IEC 27002-2015** «Информационная технология. Методы и средства обеспечения безопасности. Свод правил по средствам управления защитой информации».
- **21. СТБ ISO/IEC 27002-2012** «Информационные технологии. Методы обеспечения безопасности. Кодекс практики для менеджмента информационной безопасности».
- **22. ISO/IEC 27003:2017** «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство» (Information technology – Security techniques – Information security management systems – Guidance).

II. Создание и сопровождение систем управления информационной безопасностью

- **23. СТ РК ISO/IEC 27003-2012** «Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности».
- **24. СТБ ISO/IEC 27003-2014** «Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности».
- **25. ISO/IEC 27004:2016** «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, измерения, анализ и оценка» (Information technology – Security techniques – Information security management – Monitoring, measurement, analysis).
- **26. СТ РК ISO/IEC 27004-2012** «Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности. Измерение».
- **27. СТБ ISO/IEC 27004-2014** «Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности. Измерения».
- **28. ISO/IEC 27005:2018** «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» (Information technology – Security techniques – Information security risk management).
- **29. СТ РК ISO/IEC 27005-2013** «Информационные технологии. Методы обеспечения безопасности. Менеджмент риска информационной безопасности».
- **30. СТБ ISO/IEC 27005-2012** «Информационные технологии. Методы обеспечения безопасности. Менеджмент рисков информационной безопасности».

II. Создание и сопровождение систем управления информационной безопасностью

- **31. СТБ ISO/IEC 27006-2018** «Информационные технологии. Методы обеспечения безопасности. Требования к органам, проводящим аудит и сертификацию систем менеджмента информационной безопасности».
- **32. СТБ ISO/IEC 27011-2017** «Информационные технологии. Методы обеспечения безопасности. Руководство по менеджменту информационной безопасности для организаций телекоммуникационной отрасли на основе ISO/IEC 27002».
- **33. СТБ ISO/IEC 27035-2017** «Информационные технологии. Методы обеспечения безопасности. Менеджмент инцидентов в области информационной безопасности».
- **34. СТБ 34.101.70-2016** «Информационные технологии. Методы и средства безопасности. Методика оценки рисков информационной безопасности в информационных системах».

III. Обеспечение сетевой безопасности и обеспечение защиты веб-сервисов

- **35. ISO/IEC 27033-1:2015** «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 1. Обзор и концепции» (Information technology – Security techniques – Network security – Part 1: Overview and concepts).
- **36. СТ РК ISO/IEC 27033-1-2017** «Информационные технологии. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 1. Обзор и концепции».
- **37. ISO/IEC 27033-2:2012** «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 2. Руководящие принципы по разработке и внедрению средств обеспечения безопасности сетей» (Information technology – Security techniques – Network security – Part 2: Guidelines for the design and implementation of network security).
- **38. СТ РК ISO/IEC 27033-2-2017** «Информационные технологии. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 2. Руководящие указания по проектированию и внедрению защиты сети».
- **39. ISO/IEC 27033-3:2010** «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления» (Information technology – Security techniques – Network security – Part 3: Reference networking scenarios – Threats, design techniques and control issues).
- **40. ISO/IEC 27033-4:2018** «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 4. Коммуникации для обеспечения безопасности между сетями с применением шлюзов безопасности» (Information technology – Security techniques – Network security – Part 4: Securing communications between networks using security gateways).

III. Обеспечение сетевой безопасности и обеспечение защиты веб-сервисов

- **41. СТ РК ISO/IEC 27033-4-2017** «Информационные технологии. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 4. Коммуникации для обеспечения безопасности между сетями с применением шлюзов безопасности».
- **42. ISO/IEC 27033-5:2013** «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 5. Безопасное межсетевое взаимодействие с использованием виртуальных частных сетей (VPNs)» (Information technology – Security techniques – Network security – Part 5: Securing communications across networks using Virtual Private Networks (VPNs)).
- **43. СТ РК ISO/IEC 27033-5-2017** «Информационные технологии. Методы обеспечения безопасности. Сетевая безопасность. Часть 5. Коммуникации для обеспечения безопасности между сетями с применением виртуальных частных сетей (VPN)».
- **44. ISO/IEC 27033-6:2018** «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 6. Защищенный доступ к беспроводной IP-сети» (Information technology – Security techniques – Network security – Part 6: Securing wireless IP network access).
- **45. СТ РК ISO IEC 27033-6-2017** «Информационные технологии. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 6. Защищенный доступ к беспроводной IP-сети».
- **46. ISO/IEC 27039:2015** «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Выбор, внедрение и сопровождение систем обнаружения и предотвращения вторжений» (Information technology – Security techniques – Selection, deployment and operations of intrusion detection and prevention systems (IDPS)).
- 47. Спецификация безопасности веб-сервисов «Безопасность структурированных сообщений» (Web Services Security: **SOAP Message Security 1.1 (WS-Security 2004)**.

III. Обеспечение сетевой безопасности и обеспечение защиты веб-сервисов

- 48. Руководящие принципы по обеспечению доступности веб-контента (**Web Content Accessibility Guidelines (WCAG) 2.1**).
- **49. СТ РК ИСО/МЭК 18028-4-2007** «Технологии информационные. Методы обеспечения защиты. Защита сети информационных технологий. Часть 4. Защита удаленного доступа».
- **50. СТБ 34.101.8-2006** «Информационные технологии. Методы и средства безопасности. Программные и программно-аппаратные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования».
- **51. СТБ 34.101.14-2017** «Информационные технологии. Методы и средства безопасности. Программные средства маршрутизатора. Общие требования».
- **52. СТБ 34.101.37-2017** «Информационные технологии и безопасность. Методы и средства безопасности. Системы управления сайта. Общие требования».
- **53. СТБ 34.101.73-2017** «Информационные технологии. Методы и средства безопасности. Межсетевые экраны. Общие требования».
- **54. СТБ 34.101.74-2017** «Информационные технологии. Системы сбора и обработки данных событий информационной безопасности. Общие требования».
- **55. СТБ 34.101.75-2017** «Информационные технологии. Системы обнаружения и предотвращения вторжений. Общие требования».
- **56. СТБ 34.101.76-2017** «Информационные технологии. Методы и средства безопасности. Системы обнаружения и предотвращения утечек информации из информационных систем. Общие требования».

IV. Обеспечение защиты информации с использованием средств криптографической защиты

- 57. Спецификация безопасности на транспортном уровне **TLS 1.2: RFC 5246** (A Transport Layer Security (TLS) Protocol Version 1.2).
- 58. Спецификация безопасности на транспортном уровне **TLS 1.3: RFC 8446** (The Transport Layer Security (TLS) Protocol Version 1.3).
- 59. **Набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IPSec:** RFC 2401, RFC 2402, RFC 2403, RFC 2404, RFC 2405, RFC 2406, RFC 2407, RFC 2408, RFC 2409, RFC 2410, RFC 2411, RFC 2412.
- **60. ГОСТ 34.12-2018** «Информационная технология. Криптографическая защита информации. Блочные шифры».
- **61. ГОСТ 34.13-2018** «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров».
- **62. Рекомендации по стандартизации Р 1323565.1.020-2018** «Информационная технология. Криптографическая защита информации. Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)».
- **63. Рекомендации по стандартизации Р 1323565.1.022-2018** «Информационная технология. Криптографическая защита информации. Функции выработки производного ключа».
- **64. Рекомендации по стандартизации Р 1323565.1.017-2018** «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования».

IV. Обеспечение защиты информации с использованием средств криптографической защиты

- **65. Рекомендации по стандартизации Р 1323565.1.005-2017** «Информационная технология. Криптографическая защита информации. Допустимые объемы материала для обработки на одном ключе при использовании некоторых вариантов режимов работы блочных шифров в соответствии с ГОСТ Р 34.13-2015».
- **66. Рекомендации по стандартизации Р 1323565.1.004-2017** «Информационная технология. Криптографическая защита информации. Схемы выработки общего ключа с аутентификацией на основе открытого ключа».
- **67. Рекомендации по стандартизации Р 50.1.114-2016** «Информационная технология. Криптографическая защита информации. Параметры эллиптических кривых для криптографических алгоритмов и протоколов».
- **68. Рекомендации по стандартизации Р 50.1.113-2016** «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования».
- **69. СТБ 34.101.47-2017** «Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел».
- **70. СТБ 34.101.60-2014** «Информационные технологии и безопасность. Алгоритмы разделения секрета».
- **71. СТБ 34.101.66-2014** «Информационные технологии и безопасность. Протоколы формирования общего ключа на основе эллиптических кривых».

V. Обеспечение возможности использования электронной цифровой подписи (электронной подписи) и обеспечение функционирования сервисов доверенной третьей стороны

- 72. Спецификация управления ключами XML-подписей (**XML Key Management Specification (XKMS 2.0)** Version 2.0 W3C Recommendation 28 June 2005).
- **73. ITU-T X.842** «Информационные технологии. Методы защиты. Руководящие указания по применению и управлению службами доверенной третьей стороны» (Information technology – Security techniques – Guidelines for the use and management of trusted third party services).
- **74. ITU-T X.509** «Информационные технологии. Взаимосвязь открытых систем. Справочник: Структуры сертификатов открытых ключей и атрибутов» (Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks).
- 75. Синтаксис и обработка электронной подписи в XML (**XML Signature Syntax and Processing (Second Edition) (XML-DSig)**).
- 76. Расширение электронной подписи в XML (**XML Advanced Electronic Signatures (XAdES)**).
- 77. Расширение электронной подписи в PDF (**PDF Advanced Electronic Signatures (PadES)**).
- 78. CMS расширение электронной подписи (**CMS Advanced Electronic Signatures (CadES)**).
- **79. RFC 5280** «Профили сертификатов и списков отозванных сертификатов в инфраструктуре открытых ключей Internet X.509» (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile).
- **80. RFC 6818** «Дополнение к профилям сертификатов и списков отозванных сертификатов в инфраструктуре открытых ключей Internet X.509» (Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile).

V. Обеспечение возможности использования электронной цифровой подписи (электронной подписи) и обеспечение функционирования сервисов доверенной третьей стороны

- **81. RFC 4210** «Протокол управления сертификатами в инфраструктуре открытых ключей Internet X.509» (Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)).
- **82. PKCS#11** «Интерфейс взаимодействия с криптографическими токенами» (PKCS#11 Cryptographic Token Interface).
- **83. ГОСТ Р 34.10-2012** «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
- **84. СТБ 34.101.45-2013** «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых».
- **85. ГОСТ Р 34.11-2012** «Информационная технология. Криптографическая защита информации. Функция хэширования».
- **86. СТБ 34.101.31-2011** «Информационные технологии и безопасность. Криптографические алгоритмы шифрования и контроля целостности».
- **87. ГОСТ 34.10-2018** «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
- **88. ГОСТ 34.11-2018** «Информационная технология. Криптографическая защита информации. Функция хэширования».
- **89. Рекомендации по стандартизации Р 1323565.1.023-2018** «Информационная технология. Криптографическая защита информации. Использование алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 в сертификате, списке аннулированных сертификатов (CRL) и запросе на сертификат PKCS #10 инфраструктуры открытых ключей X.509».

V. Обеспечение возможности использования электронной цифровой подписи (электронной подписи) и обеспечение функционирования сервисов доверенной третьей стороны

- **90. СТБ 34.101.17-2012** «Информационные технологии и безопасность. Синтаксис запроса на получение сертификата».
- **91. СТБ 34.101.18-2009** «Информационные технологии. Синтаксис обмена персональной информацией».
- **92. СТБ 34.101.19-2012** «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей».
- **93. СТБ 34.101.23-2012** «Информационные технологии и безопасность. Синтаксис криптографических сообщений».
- **94. СТБ 34.101.26-2012** «Информационные технологии и безопасность. Онлайновый протокол проверки статуса сертификата (OCSP)».
- **95. СТБ 34.101.48-2012** «Информационные технологии и безопасность. Требования к политике применения сертификатов удостоверяющих центров».
- **96. СТБ 34.101.65-2014** «Информационные технологии и безопасность. Протокол защиты транспортного уровня (TLS)».
- **97. СТБ 34.101.67-2014** «Информационные технологии и безопасность. Инфраструктура атрибутных сертификатов».
- **98. СТБ 34.101.77-2016** «Информационные технологии и безопасность. Алгоритмы хэширования».
- **99. СТБ 34.101.78-2018** «Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей».

V. Обеспечение возможности использования электронной цифровой подписи (электронной подписи) и обеспечение функционирования сервисов доверенной третьей стороны

- **100. СТБ 34.101.79-2018** «Информационные технологии и безопасность. Криптографические токены».
- **101. СТБ 34.101.80-2018** «Информационные технологии и безопасность. Расширенные электронные цифровые подписи».
- **102. СТБ 34.101.81-2018** «Информационные технологии и безопасность. Протоколы службы заверения данных».
- **103. СТБ 34.101.82-2018** «Информационные технологии и безопасность. Протокол простановки штампа времени».

VI. Обеспечение доверия к цифровым сервисам

- **104. ISO 19011:2018** «Руководство по аудиту систем менеджмента» (Guidelines for auditing management systems).
- **105. СТБ 34.101.27-2011** «Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации».

VII. Обеспечение функций по идентификации субъектов электронного взаимодействия, в том числе сервисов информационно-коммуникационных технологий, и проверке правомочий

- **106. ISO/IEC 9594-8:2017** «Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 8. Структура сертификата на открытый ключ и атрибуты» (Information technology – Open Systems Interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks).
- **107. RFC 5755** «Профиль атрибутивного сертификата для авторизации» (An Internet Attribute Certificate Profile for Authorization).

Защита информации

Тема: Правовое и нормативное обеспечение защиты информации (Законодательство РБ)

Благодарю за внимание

КУТУЗОВ Виктор Владимирович

Список использованных источников

1. Рабочая программа дисциплины «Защита информации» / Кутузов В.В. – Могилев : Белорусско-Российский университет, 2019
2. Фотографии и картинки взяты с сайтов Яндекс.Картинки и Гугл.Картинки, иконки с flaticon.com
3. Конституция Республики Беларусь 1994 года (с изменениями и дополнениями, принятыми на республиканских референдумах 24 ноября 1996 г. и 17 октября 2004 г.) https://pravo.by/pravovaya-informatsiya/normativnye-dokumenty/konstitutsiya-respubliki-belarus/
4. КОНЦЕПЦИЯ национальной безопасности Республики Беларусь (Указ Президента Республики Беларусь от 9 ноября 2010 г. № 575) https://pravo.by/document/?guid=3871&p0=P31000575
5. Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» https://pravo.by/document/?guid=3871&p0=h10800455
6. Закон Республики Беларусь от 19 июля 2010 г. N 170-З «О государственных секретах» http://kgb.by/ru/zakon170-3/
7. Указ Президента Республики Беларусь от 25 февраля 2011 г. № 68 «О некоторых вопросах в сфере государственных секретов» http://kgb.by/ru/ukaz68
8. Постановление Совета Министров Республики Беларусь от 25 января 2019 г. № 53 «О допуске граждан к государственным секретам» http://kgb.by/ru/post400
9. Нормативные правовые акты регламентирующие деятельность КГБ РБ http://kgb.by/ru/normat-prav-akty-ru/

Список использованных источников

10. Постановление Совета Министров РБ от 12 августа 2014 г. № 783 «О служебной информации ограниченного распространения и информации, составляющей коммерческую тайну» https://pravo.by/document/?guid=3871&p0=C21400783&p1=1
11. Постановление Комитета государственной безопасности Республики Беларусь от 17 декабря 2018 г. № 17 «Об утверждении Инструкции о порядке выдачи разрешений на осуществление деятельности с использованием государственных секретов» http://kgb.by/ru/instrukc-gs
12. Оперативно-аналитический центр при Президенте Республики Беларусь https://oac.gov.by/
13. Законы Республики Беларусь https://oac.gov.by/law/laws-of-the-republic-of-belarus
14. Указы Президента Республики Беларусь https://oac.gov.by/law/decrees-of-the-president-of-the-republic-of-belarus
15. Постановления Совета Министров Республики Беларусь https://oac.gov.by/law/resolutions-of-the-council-of-ministers-of-the-republic-of-belarus
16. Постановления Оперативно-аналитического центра при Президенте Республики Беларусь https://oac.gov.by/law/resolutions-of-the-oac
17. Приказы Оперативно-аналитического центра при Президенте Республики Беларусь https://oac.gov.by/law/orders-of-the-oac
18. ТР 2013/027/BY «Информационные технологии. Средства защиты информации. Информационная безопасность» http://www.government.by/upload/docs/file0bcd50754d1e60d7.PDF