## Учреждение образования

## Белорусский государственный технологический университет

Кафедра полиграфического оборудования и

системы обработки информации

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 10**

Тема

«Стандарты безопасности»

по дисциплине «Стандартизация и сертификация

информационных систем и технологий»

Выполнил студент

ФИТ 4 курс 7 группа Бобрович Г.С.

Проверил

кандидат технических наук

Сулим П.Е.

Отчет по лабораторной работе

защищен с отметкой баллов

Минск 2024

СТАНДАРТЫ БЕЗОПАСНОСТИ

Найти отечественные стандарты в области безопасности информационных систем. Провести их сравнительный анализ.

##### [**ТР 2013/027/BY, BY.**](https://rlst.by/informational-resources/virtualnye-vystavki/arhiv-tematicheskih-vystavok-normativno-tehnicheskih-dokumentov/standarty-v-oblasti-zashhity-informatsii/)

##### **Информационные технологии. Средства защиты информации. Информационная безопасность : технический регламент Республики Беларусь : утв. Советом Министров Респ. Беларусь 15.05.2013 № 375 (в ред. постановления Совета Министров Респ. Беларусь 12.03.2020 № 145): введ. 01.01.2014. — Минск, 2020. — II, 6 с.**

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

##### [**СТБ 34.101.30-2017, BY.**](https://rlst.by/informational-resources/virtualnye-vystavki/arhiv-tematicheskih-vystavok-normativno-tehnicheskih-dokumentov/standarty-v-oblasti-zashhity-informatsii/)

##### **Информационные технологии. Методы и средства безопасности. Информационные системы. Классификация. — Взамен СТБ 34.101.30-2007; введ. 01.10.17. — Минск, 2017. — ІІ, 6 с.**

Стандарт устанавливает классификацию информационных систем. Стандарт распространяется на информационные системы. Стандарт обеспечивает единый методологический подход к классификации информационных систем с учетом вида обрабатываемой информации и организации на них вычислительного процесса.

##### [**СТБ 34.101.31-2020, BY.**](https://rlst.by/informational-resources/virtualnye-vystavki/arhiv-tematicheskih-vystavok-normativno-tehnicheskih-dokumentov/standarty-v-oblasti-zashhity-informatsii/)

##### **Информационные технологии и безопасность. Алгоритмы шифрования и контроля целостности. — Взамен СТБ 34.101.31-2011; введ. 01.09.21. — Минск, 2020. — ІІІ, 32 с. : табл. — Попр. (ИУ ТНПА № 1-2021).**

Стандарт устанавливает криптографические алгоритмы шифрования и контроля целостности, а также служебные алгоритмы управления ключами. Стандарт применяется при разработке средств криптографической защиты информации.

##### [**СТБ 34.101.47-2017, BY.**](https://rlst.by/informational-resources/virtualnye-vystavki/arhiv-tematicheskih-vystavok-normativno-tehnicheskih-dokumentov/standarty-v-oblasti-zashhity-informatsii/)

##### **Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел. — Взамен СТБ 34.101.47-2012; введ. 01.09.17. — Минск, 2017. — ІІ, 18 с.**

Стандарт устанавливает криптографические алгоритмы генерации псевдослучайных чисел. Алгоритмы стандарта могут применяться для построения ключей, синхропосылок, одноразовых паролей, других непредсказуемых или уникальных параметров криптографических алгоритмов и протоколов. Стандарт применяется при разработке, испытаниях и эксплуатации средств криптографической защиты информации.

##### [**СТБ 34.101.72-2018, BY.**](https://rlst.by/informational-resources/virtualnye-vystavki/arhiv-tematicheskih-vystavok-normativno-tehnicheskih-dokumentov/standarty-v-oblasti-zashhity-informatsii/)

##### **Информационные технологии. Методы и средства безопасности. Технические средства обработки информации. Классификация угроз безопасности, связанных с наличием закладных устройств и недекларированных функций. — Взамен СТБ П 34.101.72-2015; введ. 01.08.18. — Минск, 2018. — ІІ, 10 с.**

Стандарт устанавливает классификацию угроз безопасности, связанных с наличием закладных устройств и (или) недекларированных функций в технических средствах, предназначенных для обработки информации, подлежащей защите в соответствии с законодательством Республики Беларусь, в том числе информации, распространение и (или) предоставление которой ограничено (защищаемая информация), на объектах информатизации. Стандарт распространяется на средства вычислительной техники, средства и системы связи, средства записи, усиления и воспроизведения звука, переговорные и телевизионные устройства, средства изготовления и размножения документов, кинопроекционную аппаратуру и другие технические средства, связанные с приемом, накоплением, хранением, поиском, преобразованием, отображением и (или) передачей информации по каналам связи и др. Требования стандарта применяют при: разработке политики информационной безопасности организации, эксплуатирующей технические средства обработки информации, для идентификации активов и угроз, оценки рисков безопасности организации в целях принятия решения о необходимости принятия мер (применения средств управления) согласно требованиям СТБ ISO/IEC 27001; реализации мер защиты информации на объектах информатизации от угроз безопасности, связанных с наличием закладных устройств и (или) недекларированных функций в технических средствах обработки информации, согласно требованиям; разработке и актуализации обобщенной модели угроз применения закладных устройств и недекларированных функций в технических средствах обработки информации; разработке и актуализации частных моделей угроз применения закладных устройств и недекларированных функций в конкретных технических средствах обработки информации.

##### [**СТБ 34.101.73-2017, BY.**](https://rlst.by/informational-resources/virtualnye-vystavki/arhiv-tematicheskih-vystavok-normativno-tehnicheskih-dokumentov/standarty-v-oblasti-zashhity-informatsii/)

##### **Информационные технологии. Методы и средства безопасности. Межсетевые экраны. Общие требования. — Введ. 01.01.18. — Минск, 2017. — ІІ, 7 с. — Попр. (ИУ ТНПА № 9-2017). — Введен впервые.**

Стандарт распространяется на программные и программно-аппаратные средства межсетевого экранирования. Стандарт устанавливает общие требования к межсетевым экранам (МЭ). Стандарт применяется при сертификационных испытаниях, проведении испытаний в рамках государственной экспертизы для оценки соответствия требованиям стандарта, а также может быть применен при разработке МЭ.

##### [**СТБ 34.101.74-2017, BY.**](https://rlst.by/informational-resources/virtualnye-vystavki/arhiv-tematicheskih-vystavok-normativno-tehnicheskih-dokumentov/standarty-v-oblasti-zashhity-informatsii/)

##### **Информационные технологии. Система сбора и обработки данных событий информационной безопасности. Общие требования. — Введ. 01.10.17. — Минск, 2017. — II, 6 с. — Введен впервые.**

Стандарт распространяется на программные и программно-аппаратные системы сбора и обработки данных событий информационной безопасности. Стандарт устанавливает классификацию и общие требования к системам сбора и обработки данных событий информационной безопасности. Стандарт применяется при сертификационных испытаниях, проведении испытаний в рамках государственной экспертизы для оценки соответствия требованиям стандарта, а также может быть применен при разработке систем сбора и обработки данных событий информационной безопасности.

##### [**СТБ 34.101.78-2019, BY.**](https://rlst.by/informational-resources/virtualnye-vystavki/arhiv-tematicheskih-vystavok-normativno-tehnicheskih-dokumentov/standarty-v-oblasti-zashhity-informatsii/)

##### **Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей. — Введ. 01.10.19. — Минск, 2019. — IV, 43, [1] с. : ил., табл. — Введен впервые. — Попр. (ИУ ТНПА № 9-2020).**

Стандарт устанавливает профиль инфраструктуры открытых ключей, рекомендуемый для использования в Республике Беларусь. В стандарте определяются стороны инфраструктуры, процессы их взаимодействия, протоколы взаимодействия, уточняются форматы объектов инфраструктуры. Стандарт применяется при разработке средств криптографической защиты информации и информационных систем, в которых используются открытые ключи.

##### [**СТБ 34.101.81-2019, BY.**](https://rlst.by/informational-resources/virtualnye-vystavki/arhiv-tematicheskih-vystavok-normativno-tehnicheskih-dokumentov/standarty-v-oblasti-zashhity-informatsii/)

##### **Информационные технологии и безопасность. Протоколы службы заверения данных. — Введ. 01.10.19. — Минск, 2019. — ІІІ, 14 с. — Введен впервые. — Попр. (ИУ ТНПА № 9-2020).**

Стандарт устанавливает протоколы службы заверения данных, с помощью которых удостоверяются факты владения данными, существования данных, действительности электронных документов и сертификатов открытых ключей. Стандарт определяет форматы запроса к службе и соответствующего ответа, правила создания и обработки запроса и ответа. Стандарт применяется при разработке, испытаниях и эксплуатации средств и систем криптографической защиты информации, используемых в инфраструктурах открытых ключей.

##### [**СТБ ISO/IEC 27006-2018, BY.**](https://rlst.by/informational-resources/virtualnye-vystavki/arhiv-tematicheskih-vystavok-normativno-tehnicheskih-dokumentov/standarty-v-oblasti-zashhity-informatsii/)

##### **Информационные технологии. Методы обеспечения безопасности. Требования к органам, проводящим аудит и сертификацию систем менеджмента информационной безопасности. — Взамен СТБ ISO/IEC 27006-2014; введ. 01.05.18. — Минск, 2018. — V, 35 с. — Попр. (ИУ ТНПА № 4-2018).**

Стандарт конкретизирует требования и предоставляет руководство для органов, проводящих аудит и сертификацию системы менеджмента информационной безопасности (СМИБ), в дополнение к требованиям, содержащимся в ISO/IEC 17021-1 и ISO/IEC 27001. Стандарт, в первую очередь, предназначен для поддержки аккредитованных органов по сертификации, проводящих сертификацию СМИБ. Любому органу, проводящему сертификацию СМИБ, необходимо продемонстрировать соответствие требованиям, содержащимся в стандарте, с точки зрения компетентности и надежности, а содержащееся в стандарте руководство, предоставляет дополнительную интерпретацию этих требований для любого органа, проводящего сертификацию СМИБ. Стандарт может использоваться в качестве основополагающего документа при аккредитации, оценке равной стороной или других процессов аудита.

##### [**ГОСТ Р 51275-2006, RU.**](https://rlst.by/informational-resources/virtualnye-vystavki/arhiv-tematicheskih-vystavok-normativno-tehnicheskih-dokumentov/standarty-v-oblasti-zashhity-informatsii/)

##### **Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. — Введ. РБ 01.02.21. — Минск, 2020. — III, 7 с. — Введен впервые. — Попр. (ИУ ТНПА № 1-2021).**

Стандарт устанавливает классификацию и перечень факторов, воздействующих на безопасность защищаемой информации, в целях обоснования угроз безопасности информации и требований по защите информации на объекте информатизации. Стандарт распространяется на объекты информатизации, создаваемые и эксплуатируемые в различных областях деятельности (обороны, экономики, науки и других областях).

##### [**ГОСТ Р 51583-2014, RU.**](https://rlst.by/informational-resources/virtualnye-vystavki/arhiv-tematicheskih-vystavok-normativno-tehnicheskih-dokumentov/standarty-v-oblasti-zashhity-informatsii/)

##### **Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. — Введ. РБ 01.02.21. — Минск, 2020. — ІІІ, 14 с. : схемы. — Введен впервые. — Попр. (ИУ ТНПА № 1-2021).**

Стандарт распространяется на создаваемые (модернизируемые) информационные автоматизированные системы, в отношении которых законодательством или заказчиком установлены требования по их защите, и устанавливает содержание и порядок выполнения работ на стадиях и этапах создания автоматизированных систем в защищенном исполнении, содержание и порядок выполнения работ по защите информации о создаваемой (модернизируемой) автоматизированной системе в защищенном исполнении.

##### [**ГОСТ Р 52863-2007, RU.**](https://rlst.by/informational-resources/virtualnye-vystavki/arhiv-tematicheskih-vystavok-normativno-tehnicheskih-dokumentov/standarty-v-oblasti-zashhity-informatsii/)

##### **Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования. — Введ. РБ 01.02.21. — Минск, 2020. — IV, 35 с.: табл., схемы. — Введен впервые. — Попр. (ИУ ТНПА № 1-2021).**

Стандарт распространяется на автоматизированные системы в защищенном исполнении, предназначенные для защиты от преднамеренных воздействий на информацию в целях ее уничтожения, искажения или блокирования при разработке, изготовлении и эксплуатации таких систем. Стандарт входит в комплекс стандартов «Информационная технология. Автоматизированные системы» и устанавливает дополнительные требования и положения в части создания и применения автоматизированных систем в защищенном от преднамеренных силовых электромагнитных воздействий исполнении.

Приведите выводы по содержанию работы.

**Вывод:** в ходе выполнения лабораторной работы были изучены стандарты в области информационных систем в РБ. Был проведен сравнительный анализ стандартов.