Учреждение образования

Белорусский государственный технологический университет

Кафедра полиграфического оборудования и

системы обработки информации

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 10**

по дисциплине «Стандартизация и сертификация

информационных систем и технологий»

Тема

«Стандарты безопасности»

Выполнил студент

Проверил

ст. преп. Сулим П.Е.

Отчет по лабораторной работе

защищен с отметкой баллов

Минск 2022

Цель: найти отечественные и зарубежные стандарты в области безопасности информационных систем. Провести их сравнительный анализ.

«Информационная безопасность» — это процесс обеспечения доступности, целостности и конфиденциальности информации.

Под «доступностью» понимается соответственно обеспечение доступа к информации. «Целостность» — это обеспечение достоверности и полноты информации. «Конфиденциальность» подразумевает под собой обеспечение доступа к информации только авторизованным пользователям.

**Стандарт в области безопасности информационных систем РБ:**

1. 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).

2. 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).

3. 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).

4. ISO/IEC 27001:2013 «Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (Information technology – Security techniques – Information security management systems – Requirements).

5. 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).

6. ISO/IEC 27003:2010 «Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности» (Information technology – Security techniques – Information security management system implementation guidance).

7. ISO/IEC 27004:2009 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения» (Information technology – Security techniques – Information security management – Measurement).

8. ISO/IEC 27005:2011 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» (Information technology – Security techniques – Information security risk management).

9. ISO/IEC 27033-1:2009 «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).

10. ISO/IEC 18028-4:2005 «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность информационной сети. Часть 4. Обеспечение безопасности удаленного доступа» (Information technology – Security techniques – IT network security – Part 4: Securing remote access).

11. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

12. 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).

13. ITU-T Х.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).

14. Синтаксис и обработка электронной подписи в XML (XML Signature Syntax and Processing (Second Edition) (XML-DSig)).

15. Расширение электронной подписи в XML (XML Advanced Electronic Signatures (XAdES)).

16. Спецификация безопасности веб-сервисов «Безопасность структурированных сообщений» (Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)).

**Международные стандарты в области безопасности информационных систем:**

1. [BS 7799-1:2005](https://ru.wikipedia.org/wiki/BS_7799-1) — Британский стандарт BS 7799 первая часть. BS 7799 Part 1 — Code of Practice for Information Security Management (Практические правила управления информационной безопасностью) описывает 127 механизмов контроля, необходимых для построения *системы управления информационной безопасностью* ([СУИБ](https://ru.wikipedia.org/wiki/%D0%A1%D0%9C%D0%98%D0%91)) организации, определённых на основе лучших примеров мирового опыта (best practices) в данной области. Этот документ служит практическим руководством по созданию СУИБ
2. [BS 7799-2:2005](https://ru.wikipedia.org/w/index.php?title=BS_7799-2&action=edit&redlink=1) — Британский стандарт BS 7799 вторая часть стандарта. BS 7799 Part 2 — Information Security management — specification for information security management systems (Спецификация системы управления информационной безопасностью) определяет спецификацию СУИБ. Вторая часть стандарта используется в качестве критериев при проведении официальной процедуры сертификации СУИБ организации.
3. [BS 7799-3:2006](https://ru.wikipedia.org/w/index.php?title=BS_7799-3&action=edit&redlink=1) — Британский стандарт BS 7799 третья часть стандарта. Новый стандарт в области управления рисками информационной безопасности
4. [ISO/IEC 17799:2005](https://ru.wikipedia.org/wiki/ISO/IEC_17799) — «Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности». Международный стандарт, базирующийся на BS 7799-1:2005.
5. [ISO/IEC 27000](https://ru.wikipedia.org/wiki/ISO_27000) — Словарь и определения.
6. [ISO/IEC 27001](https://ru.wikipedia.org/wiki/ISO/IEC_27001) — «Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования». Международный стандарт, базирующийся на BS 7799-2:2005.
7. [ISO/IEC 27002](https://ru.wikipedia.org/wiki/ISO/IEC_27002) — «Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности». Дата выхода — 2007 год.
8. [ISO/IEC 27005](https://ru.wikipedia.org/w/index.php?title=ISO/IEC_27005&action=edit&redlink=1) — Сейчас: BS 7799-3:2006 — Руководство по менеджменту рисков ИБ.
9. ISO/IEC 31000 — Описание подхода к риск-менеджменту без привязки к ИТ/ИБ.
10. German Information Security Agency. IT Baseline Protection Manual — Standard security safeguards (Руководство по базовому уровню защиты информационных технологий).

В качестве обобщенных показателей, характеризующих стандарты информационной безопасности и имеющих значение для всех трех сторон, предлагается использовать универсальность, гибкость, гарантированность, реализуемость и актуальность.

Универсальность стандарта определяется множеством типов ВС и областью информационных технологий, к которым могут быть корректно применены его положения. Это очень важная характеристика стандарта, ибо информационные технологии переживают период бурного развития, архитектура компьютерных систем совершенствуется, а сфера их применения постоянно расширяется. Стандарты информационной безопасности в своем развитии не должны отставать от современных информационных технологий или обходить ту или иную сферу их применения.

Под гибкостью стандарта понимается возможность и удобство его применения к постоянно развивающимся информационным технологиям и время его "устаревания". Гибкость может быть достигнута исключительно через фундаментальность требований и критериев и их инвариантность по отношению к механизмам реализации и технологиям создания ИТ–продуктов.

Однако, очевидно, что чрезмерная абстрактность требований и оторванность их от практики снижает их реализуемость.

Гарантированность определяется мощностью предусмотренных стандартом методов и средств подтверждения надежности результатов квалификационного анализа. Вначале этому вопросу не уделялось много внимания, но анализ опыта применения первых стандартов информационной безопасности показал, что для достижения поставленных целей аналитики, классификаторы должны иметь возможность обосновывать свои заключения, а разработчики нуждаются в механизмах, с помощью которых они могли бы подтвердить корректность своих притязаний и предоставить потребителям определенные гарантии.

Реализуемость – это возможность адекватной реализации требований и критериев стандарта на практике, с учетом затрат на этот процесс. Реализуемость во многом связана с универсальностью и гибкостью, но отражает чисто практические и технологические аспекты реализации положений и требований стандарта.

Актуальность отражает соответствие требований и критериев стандарта постоянно развивающемуся множеству угроз безопасности и новейшим методам, и средствам, используемым злоумышленниками. Эта характеристика, наряду с универсальностью является одной из важнейших, т. к. способность противостоять угрозам и прогнозировать их развитие фактически определяет пригодность стандарта и является решающим фактором при определении его пригодности.

**Payment Card Industry Data Security Standard** (PCI DSS) — это совокупность требований по обеспечению безопасности данных о держателях платёжных карт, которые хранятся, передаются и обрабатываются в информационных системах организаций.

Стандарт разработан Советом по стандартам безопасности индустрии платежных карт (Payment Card Industry Security Standards Council, PCI SSC), учреждённым международными платёжными системами, такими как: Visa, MasterCard, American Express, JCB и Discover.

Соответствовать стандарту обязаны организации, которые хранят, обрабатывают или передают в течение года информацию хотя бы об одной карточной транзакции или владельце платежной карты. В большинстве случаев сертификационный аудит на соответствие требованиям стандарта необходим банкам, розничным магазинам и сайтам электронной коммерции, процессинговым центрам, платежным шлюзам, хранилищам носителей резервных копий данных, организациям персонализации карт и т.д.

Несоблюдение требований стандарта предусматривает наложение штрафов, вплоть до отключения от системы процессинга международных платежных систем.

Стандарт не закреплен на законодательном уровне ни в одном государстве. Контроль осуществляют Visa и MasterCard — они отвечают за санкции и штрафы. Однако отдельные требования PCI DSS можно встретить в различных правовых документах. Так, американском штате Миннесота с 2007 года действует Plastic Card Security Act, запрещающий бизнесу хранение PIN-кодов карт клиентов.

Платёжные системы устанавливают штрафы за несоблюдение требований PCI DSS. Сумма зависит от типа компании (торговое предприятие или поставщик услуг), объёмов проводимых транзакций и повторяемости нарушения. За первый проступок Visa может назначить штраф в 50 тыс. долларов, за третий — уже 200 тыс. Санкции накладывают ежемесячно вплоть до устранения несоответствий.

Невыполнение требований PCI DSS также может рассматриваться как нарушение законов о защите персональных данных. Они зависят от юрисдикции, в которой фирма осуществляет деятельность: в Европе действует [GDPR](https://base.garant.ru/71936226/), в Беларуси – «О персональных данных» 2021 г.

PCI DSS определяет следующие шесть областей контроля и 12 основных требований по безопасности.

Построение и сопровождение защищённой сети

Требование 1: установка и обеспечение функционирования межсетевых экранов для защиты данных держателей карт.

Требование 2: неиспользование выставленных по умолчанию производителями системных паролей и других параметров безопасности.

Защита данных держателей карт

Требование 3: обеспечение защиты данных держателей карт в ходе их хранения.

Требование 4: обеспечение шифрования данных держателей карт при их передаче через общедоступные сети.

Поддержка программы управления уязвимостями

Требование 5: использование и регулярное обновление антивирусного программного обеспечения.

Требование 6: разработка и поддержка безопасных систем и приложений.

Реализация мер по строгому контролю доступа

Требование 7: ограничение доступа к данным держателей карт в соответствии со служебной необходимостью.

Требование 8: присвоение уникального идентификатора каждому лицу, имеющему доступ к информационной инфраструктуре.

Требование 9: ограничение физического доступа к данным держателей карт.

Регулярный мониторинг и тестирование сети

Требование 10: контроль и отслеживание всех сеансов доступа к сетевым ресурсам и данным держателей карт.

Требование 11: регулярное тестирование систем и процессов обеспечения безопасности.

Поддержка политики информационной безопасности

Требование 12: разработка, поддержка и исполнение политики информационной безопасности

Источники:

<https://ru.wikipedia.org/wiki/PCI_DSS>

<https://ru.wikipedia.org/wiki/Стандарты_информационной_безопасности>

<https://pravo.by/document/?guid=3871&p0=F01500112>

<https://gosstandart.gov.by/international-standards-and-eu-regulation-on-data-protection>

**Выводы:** В лабораторной работе были представлены основные отечественные и зарубежные стандарты безопасности информационных систем, рассмотрен стандарт по обеспечению безопасности данных о держателях платёжных карт PCI DSS.