СОДЕРЖАНИЕ

[Используемые сокращения 3](#_Toc136363185)

[Введение 4](#_Toc136363186)

[1 Теоретические аспекты методов анализа и аудита информационной безопасности в условиях цифровой трансформации 6](#_Toc136363187)

[1.1 Понятие аудита информационной безопасности в условиях цифровой трансформации и концепции его проведения 6](#_Toc136363188)

[1.2 Обзор программных средств для проведения аудита информационной безопасности 9](#_Toc136363189)

[1.3 Правовое регулирование информационной безопасности в банковской сфере 17](#_Toc136363190)

[2 Методика оценки и аудита информационной безопасности банка 22](#_Toc136363191)

[2.1 Характеристика ПАО «Банк ВТБ» с точки зрения обеспечения информационной безопасности 22](#_Toc136363192)

[2.2 Угрозы информационной безопасности в банковском секторе 25](#_Toc136363193)

[2.3 Методики и технологии обнаружения угроз информационной безопасности банка 29](#_Toc136363194)

[2.4 Методы защиты объектов информационной безопасности банка 31](#_Toc136363195)

[3 Практические аспекты проверки соблюдения требований, предъявляемых к информационной безопасности ПАО «Банк ВТБ» 34](#_Toc136363196)

[3.1 Характеристика автомной локальной вычислительной сети отдела банка 34](#_Toc136363197)

[3.2 Реализация методики аудита информационной безопасности 39](#_Toc136363198)

[3.3 Результат аудита информационной безопасности локальной сети ПАО «Банк ВТБ» 47](#_Toc136363199)

[Заключение 55](#_Toc136363200)

[Список используемых источников 56](#_Toc136363201)

# ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

DDoS – Distributed Denial of Service, атака типа «отказ в обслуживании»;

NGFW – Next Generation Firewall;

АРМ – Автоматизированное рабочее место;

ИС – Информационная система;

ИТ – Информационные технологии;

НСД – Несанкционированный доступ;

ПО – Программное обеспечение;

ПАО – Публичное акционерное общество;

РФ – Российская Федерация;

СКУД – Система контроля и управления доступом;

СЗИ – Система защиты информации;

СМИБ – Система менеджмента информационной безопасности;

ФСБ – Федеральная служба безопасности;

ФСТЭК – Федеральная служба по техническому и экспортному контролю.

# ВВЕДЕНИЕ

В нынешних реалиях банковский сегмент является важнейшим инструментом в руках государства, а банковская карта – незаменимой вещью, которой владеет современный человек.

Именно поэтому важно понимать то, что любая потенциальная уязвимость информационной безопасности банка – должна быть устранена до того момента, пока о ней узнают злоумышленники. В противном случае такие риски могут нести за собой многомиллионный ущерб финансовому сектору экономики, а также клиентам банков.

В связи с этим, все современные банки должны придерживаться современных стандартов информационной безопасности, а также следить за актуальностью своих информационных систем.

Для поддержания безопасности своих информационных систем многие организации, в том числе и банки проводят анализ и аудит информационной безопасности для предотвращения возможных вторжений.

Данная выпускная квалификационная работа посвящена рассмотрению методов анализа и аудита информационной безопасности на примере ПАО «Банк ВТБ».

Актуальность темы отражает необходимость постоянного совершенствования методов анализа и аудита современных банковских информационных систем в условиях цифровой трансформации. Своевременное исправление уязвимостей – ключ к успеху в защите от злоумышленников.

Целью данной работы является разработка методики аудита информационной безопасности для автономной локальной сети, используемой для видеонаблюдения и контроля управления доступом внутри организации с помощью системы, построенной на базе оборудования Bolid.

Объектом исследования является локальная сеть подразделения работников банка, состоящая из трёх АРМ и одного сервера.

Предмет исследования заключен в процессе проведения аудита автономной локальной сети работников банка, с помощью разработанной методики.

Таким образом, в соответствии с поставленной целью определен следующий список задач:

* рассмотреть теоретические аспекты методов анализа и аудита;
* рассмотреть стандарты безопасности ISO/IEC 27001 и PCI DSS;
* проанализировать деятельность организации, учет и хранение бумажных носителей;
* проанализировать требования, предъявляемые к информационной безопасности банка, а также практическое их выполнение на объекте исследования;
* проанализировать ПО и оборудование, используемое для обеспечения информационной безопасности;
* провести аудит ИС, в частности: контроль учетных записей пользователя, ОС, уровней доступа, сетевых ресурсов, журнал аудитов пользователей, отказоустойчивость системы.