**Министерство образования и науки Российской Федерации**

**федеральное государственное автономное образовательное  
учреждение высшего образования  
«Санкт-Петербургский национальный исследовательский  
университет информационных технологий, механики и оптики»**

**Факультет:** Безопасности информационных технологий

**Направление:** 10.03.01 «Информационная безопасность»

**Дисциплина**

Организация и управление службой защиты информации

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1**

Физическая и техническая защита объекта информации

**Выполнил:**

студент группы N3464

Соколов Николай Андреевич

**Преподаватель:**

Канжелев Юрий Алексеевич

Санкт-Петербург

2019 г.

**Цель работы:** обеспечить физическую и логическую защиту объекта информации в банковской сфере.

**Ход работы:**

**Объект защиты:** персональные данные сотрудников и клиентов, бухгалтерская документация и банковские операции клиентов.

Объект защиты информации – информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации. (ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»)

**Местоположение:** сервер, который находится в специализированном помещении, расположенном в отдельном помещении.

**Доступ** к серверной имеет администратор ИБ и системный администратор; сотрудники банка не имеют прав доступа к серверной.

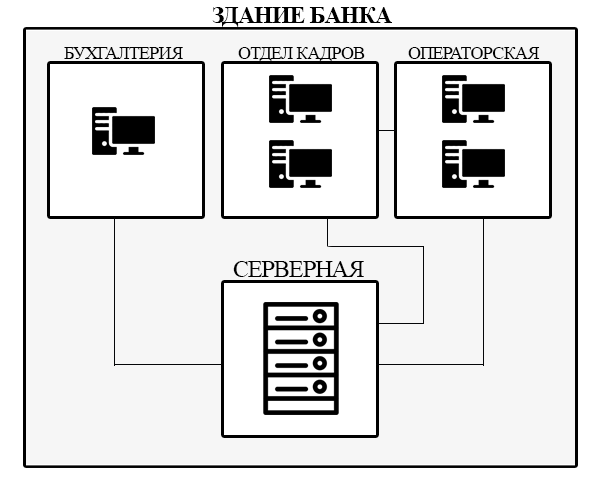


Рисунок 1 - Схема местоположения объекта защиты

**Физическая защита:**

Физическая защита информации - защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты. (ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»)

1. Для обеспечения физической защиты здания банка необходима система контроля и управления доступом (СКУД), чтобы только сотрудники компании имели возможность с помощью электронных пропусков попасть внутрь помещений банка.

2. Физический доступ к помещениям банка ограничен электронными запирающими механизмами на двери. Каждому сотруднику банка предоставляется индивидуальная идентифицирующая смарт-карта, при помощи которой сотрудник может получить доступ в бухгалтерию, отдел кадров, операторскую приложив идентификатор к считывателю карт, расположенному на двери.

3. Физический доступ в серверную ограничен еще одним специальным замком. Для доступа в помещение на смарт-карте должна быть дополнительная идентифицирующая информация, которая позволит получить доступ в серверную.

4. Защита физического доступа к серверам обеспечивается наличием железной дверей, ведением журнала регистрации посещения серверного помещения, а также установкой системы видеонаблюдения для предотвращения несанкционированного доступа. Входная дверь серверного помещения опечатывается.

5. Физическая защита персональных компьютеров сотрудников банка, достигается путем запечатывания USB-портов.

**Техническая защита:**

Техническая защита информации - защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств. (ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»)

1. Для доступа к серверу используется аутентификация: с помощью пароля или с помощью ключа.

2. Для обеспечения высокой логической защиты на сервере и на компьютерах банка должно быть установлено средство защиты информации (СЗИ), например, «Secret Net», включающее в себя следующие модули:

– защита от несанкционированного доступа;

– парольная защита;

– антивирусная защита;

– контроль доступа к ресурсам файловой системы;

– обнаружение и предотвращение вторжений;

– межсетевой экран;

– контроль устройств;

– ведение журналов событий, аудит.

3. Системный администратор должен создать для каждого сотрудника банка учетную запись, а администратор информационной безопасности (АИБ) – распределить права таким образом, чтобы только субъекты (сотрудники банка) получившие официальные разрешения (допуска) на обращение к информации имели к ней доступ.

**Вывод:** в ходе лабораторной работы была обеспечена физическая и логическая защита персональных данных в банке.