

УДК 69.04

**РЕКОМЕНДАЦИИ ИСПОЛЬЗОВАНИЯ СЛОЁВ NANOCAD
ДЛЯ РАЗДЕЛЕНИЯ ИБ-ЗОН В ПОМЕЩЕНИИ**

Веригина И.Ю., студентка гр. ИБс-231, III курс
Научный руководитель: Аксенова О.Ю., к.т.н., доцент,
доцент кафедры СКВиВ
Кузбасский государственный технический университет
имени Т.Ф. Горбачева, г. Кемерово

В условиях роста киберугроз и ужесточения требований к защите информации особую значимость приобретает комплексный подход к информационной безопасности (ИБ), включающий не только цифровые, но и физические меры защиты. Данный вопрос решается уже на стадии проектирования здания с учетом ИБ-требований, для дальнейшей аттестации помещения на соответствие требованиям защиты информации.

Важнейшим инструментом проектирования является системы автоматизированного проектирования (САПР). Однако в данных системах архитекторы и проектировщики делают акцент только на архитектурных аспектах, оставляя вопрос о распределении зон для информационной безопасности, например, такие как серверные центры с конфиденциальной информацией или комната для переговоров, куда вход доступен только определенному кругу лиц.

Проблема исследования заключается в отсутствии рекомендаций позволяющих, наглядно отображать зоны с разным уровнем доступа, согласовывать графические решения с регуляторами (ФСТЭК, ФСБ).

Целью работы является разработать рекомендации применения рабочих слоев разного цвета в САПР nanoCAD для маркировки и изображения зон с разным уровнем доступа на архитектурно-строительных чертежах административно-бытовых комплексов.

Задачи исследования:

- Проанализировать нормативные документы, предъявляемые к защищаемым помещениям.
- Определить оптимальные способы визуализации и маркировки ИБ-зон.
- Создать план помещения с учетом предлагаемой рекомендации.

Основные нормативные документы, регулирующие информационную безопасность, являются:

- Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» [1].
- Федеральный закон 27.07.2006 №152-ФЗ «О персональных данных» [2].

- Приказ ФСТЭК от 29 апреля 2021 г. N 77 об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну [3].

- Требования по безопасности информации, утвержденный приказом ФСТЭК России от 2 июня 2020 г. N 76 [4].

- Постановлением Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [5].

В указанных нормативных документах представлены требования по безопасности информации, где устанавливается 6 уровней доверия, от самого низкого шестого уровня до первого верхнего уровня, а также 4 уровня защищенности (УЗ) информационных систем персональных данных (ИС-ПДн): УЗ-4, УЗ-3, УЗ-2, УЗ-1.

Для отображения ИБ-зоны в архитектурно-строительных чертежах можно использовать рабочие слои разного цвета, при этом выполняя запись обозначений при необходимости в технических характеристиках или технических условиях. В качестве примера разберем изображение ИБ-зоны на плане офисного помещения (рис. 1).

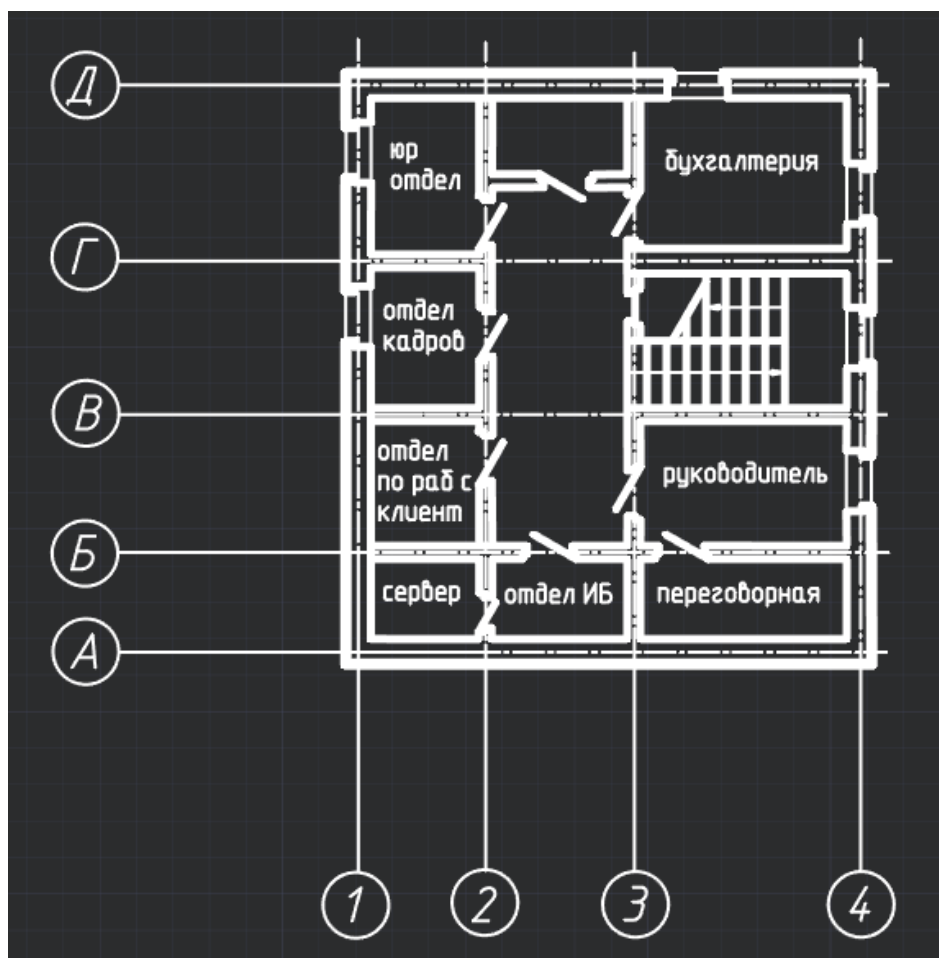


Рис. 1. План офисного помещения

Наиболее охраняемыми зонами в офисе являются серверное помещение и отдел информационной безопасности. В них обрабатываются данные, подверженные угрозам первого типа (наличие не декларированных возможностей в системном ПО). Для их обозначения на плане используется рабочий слой красного цвета (рис. 2).

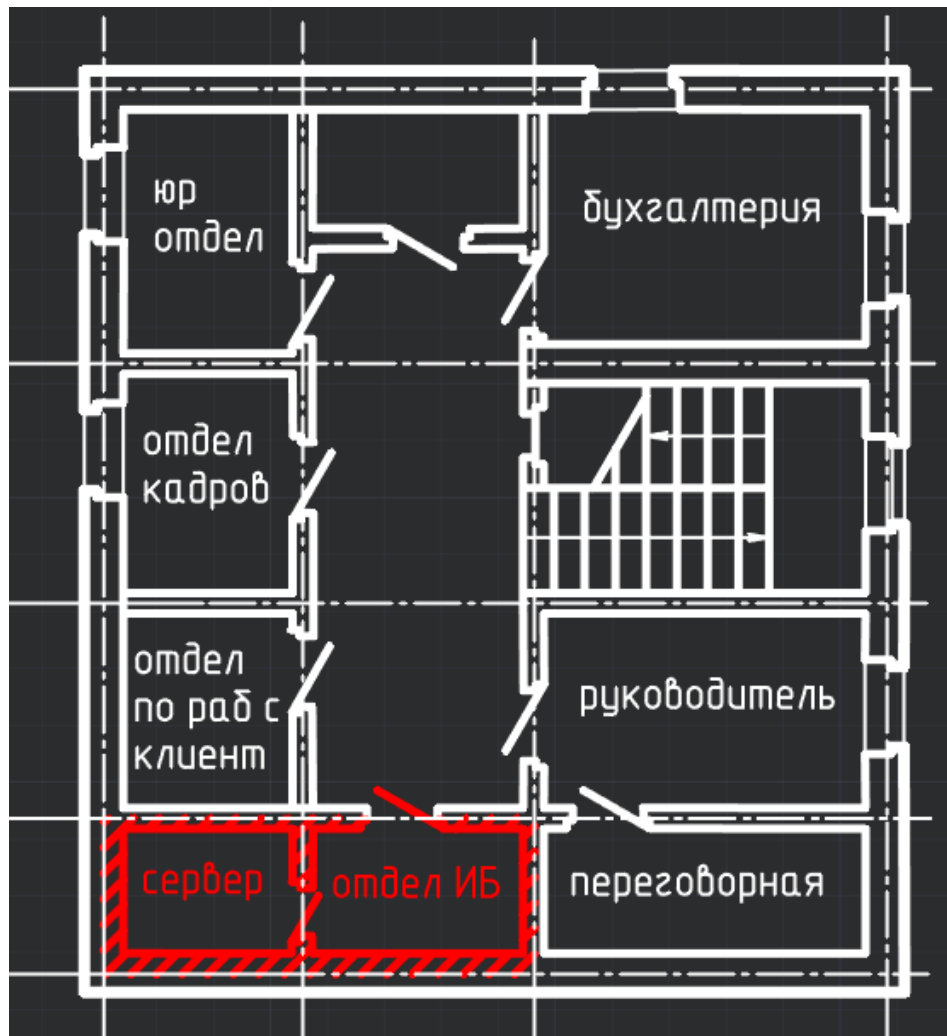


Рис. 2. Изображение на плане офисного помещения зон сервера и отдела ИБ

Отдел по работе с клиентами оперирует персональными данными 3-й и 4-й групп (общедоступные ПДн и иные категории). Угрозы для этих данных относятся к 3-му типу и не связаны с не декларированными возможностями ПО. В связи с этим данный отдел классифицируется как зона с низким уровнем риска и выделяется зелёным цветом (рис. 3).

Остальные отделы относятся ко второму типу угроз — это связано с возможностью наличия не декларированных возможностей в прикладном программном обеспечении (как общего, так и специального назначения, например, бухгалтерского). Данные помещения соответствуют УЗ-2 — уровню защищённости, при котором нарушение безопасности персональных данных

может привести к неблагоприятным последствиям для субъектов. Однако по сравнению с серверной комнатой и отделом информационной безопасности эти зоны обладают меньшим уровнем риска. Поэтому для их визуализации на плане рекомендуется использовать жёлтый цвет (см. рис. 3).

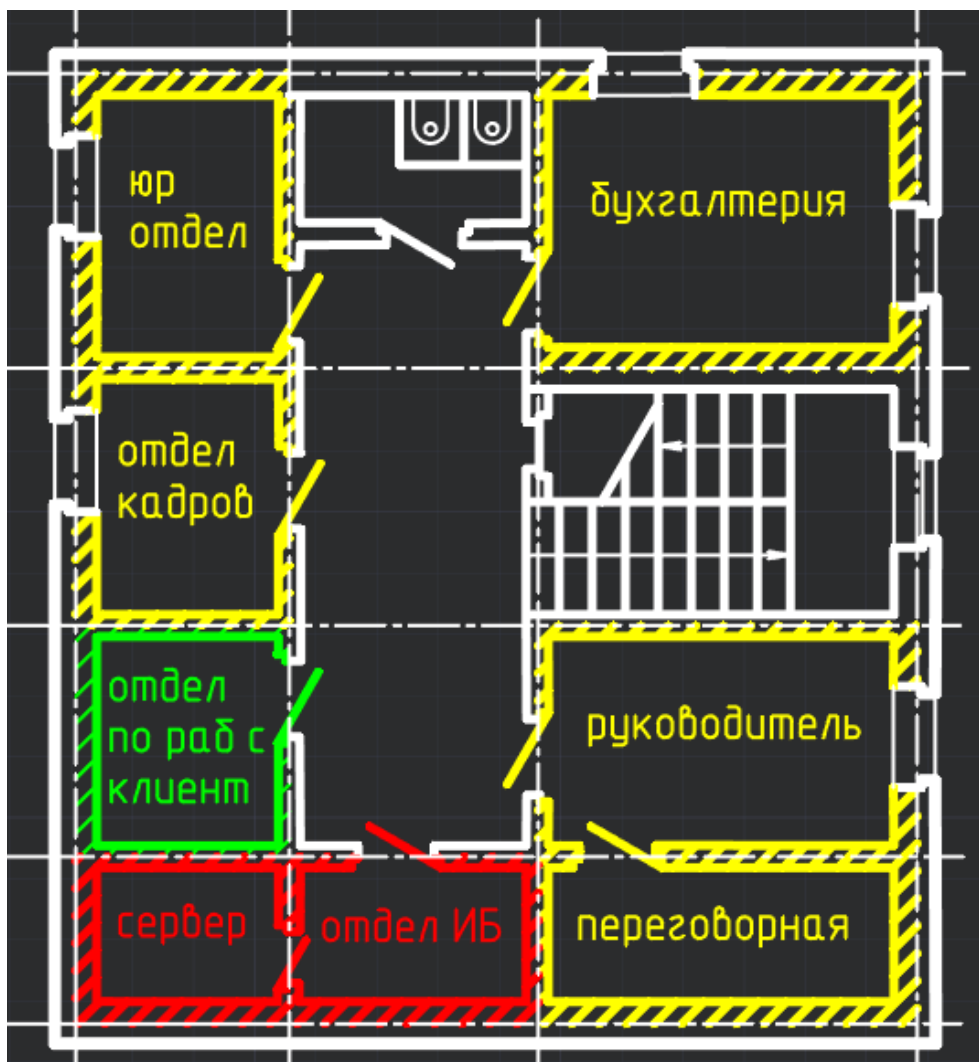


Рис. 3. Изображение на плане офисного помещения
всех ИБ-зон помещения

В ходе проведенной работы были разработаны рекомендации для маркировки и изображения на архитектурно-строительных чертежах административно-бытовых комплексов зон с различным уровнем доступа к информации с использованием рабочих слоев разного цвета в САПР nanoCAD. Предложенный подход основан на анализе действующей нормативной базы, включая федеральные законы, приказы ФСТЭК России и постановления Правительства РФ, что обеспечивает его соответствие требованиям регуляторов и позволяет использовать полученные графические решения при аттестации объектов информатизации.

В рамках работы были определены оптимальные способы цветовой маркировки ИБ-зон: красный цвет – для наиболее защищённых помещений (серверная, отдел ИБ), жёлтый – для зон со средним уровнем риска (отделы с УЗ-2) и зелёный – для зон с низким уровнем угроз. Такая дифференциация обеспечивает наглядность, упрощает проектирование и позволяет оперативно согласовывать решения с контролирующими органами.

Список литературы:

1. Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» [электронный ресурс] - URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (Дата обращения 15.03.2026).
2. Федеральный закон 27.07.2006 №152-ФЗ «О персональных данных» [электронный ресурс] - URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (Дата обращения 15.03.2026).
3. Приказ ФСТЭК от 29 апреля 2021 г. N 77 об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну [электронный ресурс] - URL: <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-29-aprelya-2021-g-n-77> (Дата обращения 15.03.2026).
4. Требования по безопасности информации, утвержденный приказом ФСТЭК России от 2 июня 2020 г. N 76 [электронный ресурс] - URL: <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/trebovaniya-po-bezopasnosti-informatsii-utverzhdenny-prikazom-fstek-rossii-ot-2-iyunya-2020-g-n-76> (Дата обращения 15.03.2026).
5. Постановлением Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [электронный ресурс] - URL: https://www.consultant.ru/document/cons_doc_LAW_137356/8c86cf6357879e861790a8a7ca8bea4227d56c72/ (Дата обращения 15.03.2026).