Ролевая модель.

В ООО "My Company" введено разграничение прав доступа к ресурсам на основе ролевой модели. Каждая роль определяет набор прав доступа к информационным ресурсам и системам обработки информации (СОИ).

**Основные роли:**

|  |  |
| --- | --- |
| **Администратор домена** | Управляет доменной инфраструктурой ООО "My Company", имеет доступ к серверу домена, DHCP и DNS. |
| **Администратор серверов** | Управляет серверными ресурсами ООО "My Company", имеет доступ к серверам и соответствующей инфраструктуре. |
| **Администратор сервисов** | Управляет ИТ сервисами ООО "My Company, управляет и предоставляет доступ |
| **Техническая поддержка** | Обеспечивает техническую поддержку сотрудников, имеет ограниченный доступ к инфраструктуре. |
| **Администратор БД** | Управляет базами данных в ООО "My Company", имеет доступ к базам данных и системам управления базами данных. Администраторы домена, Teamleads. |
| **Технические УЗ** | Обеспечивают работу систем мониторинга, СЗИ в инфраструктуре ООО "My Company" |
| **Аудит информационной безопасности** | Проводит аудит информационной безопасности, имеет доступ к сетевой инфраструктуре, конфиденциальным данным и серверам для проверки и контроля. |
| **Владелец ресурса, Teamlead, руководитель проекта** | Является владельцем определенного ресурса/проекта/базу данных с конфиденциальными данными и имеет права администратора данного ресурса. Отвечает за управление доступом ресурса/проекта/БД |
| **Разработчики** | Занимается разработкой программного обеспечения, имеет доступ ~~к базам данных клиентов~~ и коду проекта. |
| **Внедрение и консалтинг** | Выполняет расчёты и анализ данных, имеет доступ к базам данных клиентов и алгоритмам расчётов. |
| **Администрация (управление персоналом, бухгалтерия, руководство** | Выполняют административные функции управления. Занимаются обработкой, модификацией и хранением персональных данных. Имеет доступ к персональным данным сотрудников |
| **Подразделение продаж и маркетинга** | Имеют доступ только к общедоступным данным |

**Права доступа по ролям:**

* "Чтение" означает возможность просмотра данных или информации.
* "Запись" означает возможность изменения данных или информации.
* "Удаление" означает возможность удаления данных или информации.
* "Модификация" означает возможность внесения изменений в конфигурацию или настройки ресурса.
* "Владелец" означает полный контроль над ресурсом (включая управление доступом).

**Дополнительные условия доступа:**

* Доступ к конфиденциальным данным/базам данных с конфиденциальными данными только из среды/подсети разработчиков определенного IP администратора инфраструктуры.
* Доступ к персональным данным только из подсети подразделения по работе с персоналом и/или отдельно выделенных IP адресов.
* Доступ к администрированию инфраструктуры, серверам только с определенных IP адресов.
* Доступ к ресурсам может быть ограничен по IP-адресу или временным интервалам.
* Доступ к ресурсам может быть ограничен в зависимости от уровня конфиденциальности данных.

**Управление доступом:**

* Все изменения прав доступа должны быть задокументированы\зафиксированы.
* Запрос на предоставление доступа к ресурсу поступает от владельца ресурса в ИТ отдел и контролируется службой безопасности информации с помощью email, заявки в YT.
* Доступ к ресурсам регулярно пересматривается и обновляется.
* При создание нового проекта назначается его Teamlead/руководитель проекта, который отвечает за организацию доступа к ресурсам, задействованным в данном проекте.
* Все пользователи должны проходить двухфакторную аутентификацию.

Матрица доступа

В данной матрице описаны права доступа для различных ролей в организации, а также условия доступа к различным ресурсам и проектам.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Группы/Роли** | **Ресурсы** | **Чтение** | **Запись** | **Модификация** | **Удаление** | **Владелец** | **Условия доступа** |
| **Администратор домена** | Сетевая инфраструктура (AD, DHCP, DNS) | Да | Да | Да | Да | Да | Только с определённых IP. Доступ по согласованию с ИТ отделом и СБИ. |
| **Администраторы серверов** | Серверные ресурсы | Да | Да | Да | Да | Нет | Только с определённых IP. Доступ по согласованию с ИТ отделом и СБИ. |
| **Администраторы сервисов** | YT, Confluence, NC и т.д. | Да | Да | Да | Да | Да | Полный доступ к сервисам |
| **Техническая поддержка** | Рабочие станции, периферия инфраструктуры | Да | Да | Нет | Нет | Нет | Ограниченный доступ (без доступа к КИ, ПДн). |
| **Технические УЗ** | Инфраструктура (серверы, рабочие станции, БД) | Да | Нет | Нет | Нет | Нет | Для выполнения функций мониторинга, агенты СЗИ |
| **Аудит информационной безопасности** | Сетевая инфраструктура, конфиденциальные данные, сервера | Да | Нет | Нет | Нет | Нет | Только с определённых IP. Доступ для проверки и контроля. |
| **Teamlead, руководитель проекта, владелец ресурса** | Конфиденциальные базы данных, проекты | Да | Да | Да | Да | Да | Полный доступ к проекту, который он ведет. Контролирует запросы на доступ. Только из подсети разработчиков. |
| **Разработчики** | Конфиденциальные базы данных, проекты | Да | Да | Да | Нет | Нет | Только из подсети разработчиков. Доступ по запросу Teamlead и с одобрения СБИ. |
| **Разработка и исследования** | Конфиденциальные базы данных | Да | Нет | Нет | Нет | Нет | Только из подсети математиков. Доступ по запросу Teamlead и с одобрения СБИ. |
| **Администраторы инфраструктуры** | Конфиденциальные базы данных, инфраструктура | Да | Да | Да | Да | Нет | Только с определённых IP. Доступ по запросу владельца и с одобрения СБИ. |
| **Внедрение и консалтинг** | Общедоступные данные | Да | Нет | Нет | Нет | Нет | Без ограничений |
| **Подразделение продаж и маркетинга** | Общедоступные данные | Да | Нет | Нет | Нет | Нет | Без ограничений |
| **Администрация/Отдел персонала /Бухгалтерия** | Конфиденциальные базы данных, инфраструктура | Да | Нет | Нет | Нет | Нет | Доступ уровня чтение/просмотр |
| Персональные данные | Да | Да | Да | Да | Да | Только из подсети отдела кадров или определённых IP. Доступ по согласованию с владельцем и СБИ. |
| **Администрация/Отдел ИТ-инфраструктуры** | Конфиденциальные базы данных, инфраструктура | Да | Да | Да | Да | Нет | Только с определённых IP. Доступ по запросу владельца и с одобрения СБИ. |
| **Все пользователи** | Общедоступные данные | Да | Нет | Нет | Нет | Нет | Без ограничений |
| **Внешние пользователи** |  |  |  |  |  |  |  |
| **Сторонние пользователи** |  |  |  |  |  |  |  |

Пояснения к матрице. Описание ролей.

1. **Администратор домена**: имеет полный доступ к доменной инфраструктуре, включая серверы AD, DHCP, DNS. Доступ только с определённых IP-адресов и по согласованию с ИТ отделом и СБИ.
2. **Администраторы серверов**: управляют серверными ресурсами, обладают полными правами на их управление. Доступ ограничен определёнными IP-адресами и требует согласования с ИТ отделом и СБИ.
3. **Администратор сервисов**: управляет ИТ сервисами, обладают полными правами и предоставляет доступ к сервису по согласованию с владельцем/руководителем подразделения. Доступ только с определённых IP-адресов.
4. **Техническая поддержка**: имеет ограниченный доступ к серверным ресурсам и инфраструктуре, исключительно для выполнения задач поддержки. Доступ только с определённых IP-адресов.
5. **Технические УЗ**: необходимы для функционирования систем мониторинга инфраструктуры и для собора логов событий ИБ.
6. **Аудит информационной безопасности**: доступен для проверки и контроля ресурсов, включая серверы и конфиденциальные данные. Имеет только права чтения и ограничен определёнными IP-адресами.
7. **Teamlead/руководитель проектов**: отвечает за проект в среде разработки и является владельцем базы данных с конфиденциальной информацией для этого проекта. Имеет полный доступ к проекту и контролирует запросы на доступ. Контролирует доступ к ресурсам, которыми он управляет. Доступ к КИ осуществляется только из подсети разработчиков. Для доступа к УЗ добавляется префикс.
8. **Разработчики**: работают с проектами и конфиденциальными базами данных в среде разработки. Доступ предоставляется по запросу Teamlead/руководителя проектов и с одобрения СБИ. Доступ ограничен подсетью разработчиков. Для доступа к УЗ добавляется префикс.
9. **Администрация/Отдел персонала /Бухгалтерия**: выполняют функции, связанные с управлением в организации. Подразделение персонала выполняют обработку ПДн. Доступ к ПДн предоставляется из подсети отдела кадров или определённых IP. Доступ по согласованию с владельцем и СБИ.
10. **Внедрение и консалтинг**: используют общедоступные данные.
11. **Подразделение продаж и маркетинга:** используют общедоступные данные.