

[права доступа](#), [Инвентаризация](#)

# Инвентаризация: Контроль доступа

Черновик учета доступа пользователей к ресурсам.

## Access Types

Таблица типов доступа которые можно предоставить от объекта к субъекту. Вероятно надо сделать поля, к каким типам ресурсов (субъектов) применимы

ACCES_TYPES
read //для сервиса, обор.
write //для сервиса, обор.
vnc_ro //для IP, комп, обор
rdp //для IP, комп, обор
rdp обрезанный
и т.д.

## Access Control Entry

Запись о доступе конкретного объекта: пользователя, компьютера, сетевого диапазона

Конкретным способом (чтение/запись/протокол и т.п.). Способы - просто названия из списка, который можно пополнять

прикрепляется к ACL

SRC/OBJ (множеств)	Access_type
user_ids //польз. в т.ч. для контрагента	access_ids //множеств?
net_ips_ids //сетевой адрес с маской	
comp_ids //операционная система	
ACL	
acl_id	

## Access Control List

Список доступов (ACE) к какому либо ресурсу в течение какого либо времени на каком то основании

ACEs	SUBJECT/TARGET
aces_ids	service_id //сервис
	net_ips_id //сетевой адрес с маской
	comp_id //операционная система
	tech_id //оборудование??
SCHEDULE	Reason
schedule_id	Просто поле типа текст с Markdown форматированием

## Schedule

Используем стандартные объекты типа расписание, но в интерфейсе подавляем часть, обеспечивающую ежедневное и еженедельные расписания. Оставляем только периоды включения и выключения

Если расписание не объявлено - ACL действует всегда.  
Если объявлено, то только на время из расписания (по умолчанию расписание - пустое. Т.е. до добавления первого периода включения ACL не действует)

Periods
periods_ids

## Schedule Period

Собственно стандартные объекты рабочих/нерабочих периодов в расписании.

Вероятно поле комментарий надо сделать тоже в Markdown. А может хватит и так. В него нужно вносить основание для продления доступа на новый период (номер СЗ)

Period
schedule_id
is_work
period_begin
period_end
comment

Получается при получении служебки на предоставление доступа группе пользователей

- к удаленному доступу (пользователь → сервис Wireguard)
- к своему компу по RDP (пользователь,ip → ОС по RDP)

Будет порождаться грядка ACL:

- 1шт на доступ пользователей к сервису
- Nшт на доступ [VPN IP пользователя, учетки пользователя] по RDP к целевой ОС

Все они будут связаны через расписание. Что довольно странно Но получается, что в расписании есть все необходимые поля для этого и если других полей не нужно, то дополнительная сущность будет избыточной (тут приходит Оккам и угрожает бритвой)

Также получается что основание предоставления доступа можно вписывать двояко (есть поле в самом ACL и в каждом периоде предоставления)

Работать с самими ACL в чистом виде вероятно будет неудобно, хотя мало где работа с ACL идет отдельно от субъектов. В нашем случае можно будет наверно сделать таблицу

объект	доступ	субъект	активность ACL (в наст время исходя из расписания)
Пупкин	RDP обрезанный	PUPKIN-IA	активен

и по ней искать/просматривать доступы конкретных людей к конкретным ресурсам также очевидно что предоставленные доступы будет видно на страничке объекта и ресурса

Доступ к сложным объектам наверно надо будет реализовывать через ресурсы-сервисы (которые сами по себе комплексный объект, включающий в себя и ОС и оборудование и субсервисы). Ну т.е. если мы в кластер терминалов добавили еще один сервер - не должно быть необходимо переделывать все ACL. Нужно добавить сервер в сервис и все. Попробуем на первое время так ограничиваться. Если этого будет мало - там посмотрим в сторону сборных таргетов/ресурсов.

From:  
<http://wiki.reviakin.net/> - Wiki

Permanent link:

[http://wiki.reviakin.net/%D0%B8%D0%BD%D0%82%D0%85%D0%BD%D1%82%D0%80%D1%80%D0%B8%D0%87%D0%80%D1%86%D0%B8%D1%8F%D0%8A%D0%BE%D0%8D%D1%82%D1%80%D0%BE%D0%B8%D1%8C\\_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%80](http://wiki.reviakin.net/%D0%B8%D0%BD%D0%82%D0%85%D0%BD%D1%82%D0%80%D1%80%D0%B8%D0%87%D0%80%D1%86%D0%B8%D1%8F%D0%8A%D0%BE%D0%8D%D1%82%D1%80%D0%BE%D0%B8%D1%8C_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%80)

Last update: 2021/07/12 18:24

