Инструкция для администраторов ВУЗа: ПОДГОТОВИТЕЛЬНЫЕ РАБОТЫ И ТРЕБОВАНИЯ ДЛЯ ПОДКЛЮЧЕНИЯ ACTIVE DIRECTORY К HERO STUDY SPACE

ДЛЯ ВУЗОВ, КОТОРЫЕ ИСПОЛЬЗУЮТ Active Directory (ACTIVE DIRECTORY)

Для корректного подключения системы **Hero Study Space** к системе службы каталогов **Active Directory** с целью управления пользователями сети требуется:

1. Выделить со стороны ВУЗа ответственного сотрудника с навыками системного администрирования. Предоставить **контактный Email, телефон и логин в Telegram или Whatsapp** для оперативной связи.
2. Создать и настроить пользователя на стороне **Active Directory** для подключения им со стороны **Hero Study Space**.
    - Настроить **доступы для созданного пользователя на запись, чтение, изменение и удаление** данных из ряда директорий (DN) **Active Directory**.
    - Предоставить Hero Study данные (логин, пароль, адрес сервера Active Directory, DN для сотрудников, DN для студентов - желательно разные для разных уровней образ.) в **Hero Study Space.**
    - Перечень директорий (DN) должен содержать описания - какая из директорий **за что отвечает**. При этом, директории **для хранения студентов и сотрудников должны быть разными.**
3. Создать пользователя типа **“Сотрудник”** на стороне **Active Directory** с доступами как у обычного сотрудника ВУЗа (желательно управленческое звено). Предоставить **Hero Study Space** учетные данные пользователя (логин, пароль);
4. Определить правила формирования **“Логина AD”,** а соответственно и корпоративного **“Email”** для новых пользователей (студенты/сотрудники). При этом корпоративный **“Email”**, включает в себя **“Логин AD”**, но в конце содержит уникальное для ВУЗа доменное имя. При этом, желательно, правила формирования логинов делать различными для ППС и Студентов.

4.1. **Для сотрудника:**

- **1 вариант - предпочтительный**
  “Логин AD”: “И.О.Фамилия” на английском”
  Корпоративный **“Email”:** “Логин AD” + доменное имя.
  Пример: a.m.medetov@edu.university
- **2 вариант**
  “Логин AD”: “ “Фамилия.И” на английском” + доменное имя
  Корпоративный **“Email”:** “Логин AD” + доменное имя.
  Пример: a.m.medetov@edu.university

4.2. **Для студента:**

- **1 вариант - предпочтительный**
  “Логин AD”: основой для логина является поле **“IDSS”**, которое генерируется автоматически и выглядит **примерно так:** 23B32420, где, 23 - **год поступления**, B - **обозначение уровня образования**, 32420 - **нумератор**, он же ID объекта в спр-ке “Абитуриенты”. Т.е. это поле является уникальным идентификатором студента.

  Корпоративный **“Email”:** “Логин AD” + доменное имя.
  Пример: 23B32420@edu.university
- **2 вариант**
  “Логин AD”: ИИН + буква уровня образования
  Для студентов разных уровней образования (магистратура, докторантура и пр., кроме бакалавриат) будут использованы отличительные черты в логине.
  Корпоративный **“Email”:** “Логин AD” + доменное имя.

  Пример:
  150119929845 - бакалавриат
  150119929845-M@edu.university - магистратура
  150119929845-D@edu.university - докторантура
- **3 вариант**
  “Логин AD”: порядковый номер студента (ID)
  Корпоративный **“Email”:** “Логин AD” + доменное имя.
  Пример: 2345@edu.university

4.3. Ознакомиться с перечнем атрибутов пользователей **Hero Study Space** необходимо передавать/синхронизировать в **Active Directory** и на каком языке **(En/Ru).**
Перечень передаваемых атрибутов пользователей:

Имя атрибута	Описание	Формат
givenName	Имя пользователя	Кайрат
sn	Фамилия пользователя	Кайратов
distinguishedname	Директория хранения пользователя в AD	employees
mail	Адрес электронной почты пользователя	kairatov.a@univer.edu.kz
displayName	Имя пользователя для вывода	Кайрат Кайратов
cn	Общее имя пользователя	kairatov.a
targetAddress	Адрес электронной почты пользователя	kairatov.a@univer.edu.kz
proxyAddresses -	"SMTP:" + mail	SMTP:kairatov.a@univer.edu.kz
department	Отдел пользователя	Отдел системного администрирования
company	Организация пользователя	Университет
userPrincipalName	Имя пользователя системы в формате адреса электронной почты	kairatov.a@univer.edu.kz
sAMAccountName	givenName + sn в виде транслита	Kairat Kairatov
password	Пароль	23Neb2fd

Для того чтобы студентов и действующих сотрудников можно было корректно мигрировать из исторической системы с теми же логинами, какие им были присвоены ранее, необходимо

4.4. **Исследовать историческую ERP-систему** ВУЗа на предмет наличия в исторической системе (Univer, Sirius и пр.) **логина (корпоративные “Email”)**;
4.5. Уточнить **по какому полю** можно сопоставить эти логины с карточкой **сотрудника/студента** в системе **Active Directory** или **Hero Study Space**. К примеру, сопоставление может происходить по полю “ИИН”.
4.6. Предоставить **Hero Study Space доступ** к БД **исторической ERP-системы** и Active Directory, позволяющий **мигрировать** данные студентов и сотрудников.

Шаблон формы для обмена данными - см. ниже.

Форма обмена данными для подключения AD к Hero Study

Контактная информация

Контактная информация	Hero	Клиент
ФИО	Кучковский Юрий	
Email	yury.kuchkovskiy@hero.study	
Рабочий тел.		
Мобильный тел.	+77014379469	

Параметры VPN (заполняются при необходимости)

Информация VPN	VPN Hero	VPN (Клиент)
Название		
IP адрес-внешний	94.247.135.70	
IP адрес-внутренний	192.168.99.15	
ОС	Ubuntu 18.04	
Название ПО	Strongswan	
Версия ПО	5.6.2	

-

Параметры IPsec

Данные туннеля		VPN Hero	VPN (Клиент)
Фаза 1	Authentication Method	PSK	
	Encryption Scheme	IKEv2	
	Diffie-Hellman Group	Group14	
	Cryptography Algorithm	AES256	
	Hash Algorithm	SHA256	
	Lifetime (for renegotiation)	86400 sec	
Фаза 2	Encapsulation (ESP or AH)	ESP	
	Encryption Algorithm	AES256	
	Authentication Algorithm	SHA256	
	Lifetime (for renegotiation)	3600 sec	
PSK			

Параметры для соединения с LDAP сервером:

Параметр:	Значение (пример):
LDAP_HOST	ldap://154.44.606.34:525
LDAP_INITIAL_USER_DN	CN=heroadm Study,CN=Users,DC=domain,DC=qyzpu,DC=edu,DC=kz
LDAP_USER	univer\heroadm
LDAP_INITIAL_USER_PASSWORD	p2Y6u3Sea
OU для сотрудников	OU=employees,OU=univer,DC=domain,DC=univer,DC=edu,DC=kz
OU для студентов	OU=students,OU=univer,DC=domain,DC=univer,DC=edu,DC=kz