

Медицински университет – Плевен

Анализ

Извършване на цялостен анализ на наличната ИТ инфраструктура

„ЕМ УАЙ Синерджи“ ООД

История на промените

Дата	Версия	Създаден от	Описание
26.08.2021	1.0	Ростислав Русинов	Първоначална версия

Съдържание

1. Речник на термини, дефиниции и съкращения	4
1.1. Използвани акроними	4
2. Въведение	4
2.1. Цел на документа	4
2.2. Информация за Възложителя	5
2.3. За проекта	5
2.4. Контакти	5
2.4.1. От страна на Възложителя	5
2.4.2. От страна на Изпълнителя	5
3. Текущо състояние	6
3.1. Хардуерен слой	6
3.1.1. Servers	6
3.1.2. Дискови масиви	6
3.1.3. Комуникационно оборудване	6
3.1.4. Клиенти и периферия	8
3.2. Инфраструктурен софтуерен слой	9
3.2.1. Microsoft лицензи за SaaS	9
3.2.2. Електронна поща	10
3.2.3. Файлови сървъри	10
3.2.4. Активна Директория	11
3.2.5. Антивирусна защита	11
3.2.6. Биометрична идентификация	11
3.2.7. Наблюдение на инфраструктурата	11
3.3. Инфраструктурен мрежови слой	11
3.4. Приложен софтуер	13
3.4.1. HR и счетоводен софтуер	13
3.4.2. Деловодна система	13
3.4.3. Информационна система за управление на образованието	13
3.4.4. Дистанционно обучение	14
3.4.5. Библиотечен каталог	15
3.5. Сигурност	15
3.6. Непрекъсваемост на системите	16
3.6.1. Резервираност на сървъри и приложения	16
3.6.2. Резервираност на мрежа	16
3.6.3. Архивиране на системите	16

4. Констатации по текущото състояние	17
5. Визия и препоръки	20
5.1. Визия.....	20
5.2. Дизайн	20
5.2.1. Ограничения и зависимости при изпълнение на дизайн	21
5.2.2. Дизайн на високо ниво.....	21
5.2.3. Дизайн на сървърна инфраструктура	23
5.2.4. Дизайн на мрежова инфраструктура	24
5.3. Инициативи	24
5.4. Пътна карта.....	26
6. Заключение	26
Приложение 1	0

1. Речник на термини, дефиниции и съкращения

1.1. Използвани акроними

Акроним	Описание
ВМ	Виртуална машина
ИСУ	Интегрирана система за управление
ОС	Операционна система
СКС	Структурно кабелна система
СУСИ	Система за управление на сигурността
СУБД	Система за Управление на Бази от Данни
ЦИО	Център за Информационно Обслужване към Медицински университет – Плевен
AAD	Azure Active Directory
AD	Майкрософт Active Directory
BREN	Bulgarian Research and Education Network
BYOD	Bring your own device
CPU	Central Processing Unit
DC	Domain Controller
EOS	End of support / Край на поддръжка
HBA	Host Bus Adapter
IaaS	Infrastructure as a service / Инфраструктура като услуга
M365	Майкрософт 365 Business
MFA	Multi Factor Authentication
NGF	Next-generation firewall
ODF	Optical Distribution Frame
RU	Rack Unit
RTO	Recovery Time Objective
RPO	Recovery Point Objective
VLAN	Virtual Local Area Network
UPN	User principle name
UPS	Uninterruptible power supply
SaaS	Software as a service
SIEM	Security information and event management
SIS	School Information System
SSID	Service Set Identifier
SSO	Single Sign On
SLA	Service level agreement
STaaS	Storage as a service / Дисков ресурс като услуга

2. Въведение

2.1. Цел на документа

Настоящият документ по проект „Извършване на цялостен анализ на наличната ИТ инфраструктура“ има за цел да представи в резюме състоянието на информационната структура, ресурсната обезпеченост на информационните процеси, свързаните с тях ресурси за осигуряване на информацията и други процеси, свързани с информационните системи. На базата на анализа ще бъдат формулирани предложения за надграждане и подобряване, съгласно добрите практики, стандарти и законови рамки. Резултатите от анализа ще предоставят възможност на ръководството на Медицински университет – Плевен за създаването на ясен и точен план за

действие, вземане на информирани решения и приоритизиране на дейностите, спрямо текущото състояние на инфраструктурата.

2.2. Информация за Възложителя

Медицински университет – Плевен е автономно, държавно, висше училище със статут на юридическо лице и предмет на дейност:

- подготовка на кадри с висше медицинско образование – магистри, бакалаври, професионални бакалаври;
- подготовка на докторанти за придобиване на образователната и научна степен “доктор”;
- следдипломно обучение на висши медицински и немедицински кадри за придобиване на специалност и продължително обучение;
- развитие на науката, културата и иновационната дейност;
- фундаментални и приложни научни изследвания;
- консултативна и експертна дейност;
- международна интеграция в образованието и науката;
- информационна, административна, социална, спортна, издателска и други дейности.

Име	Медицински университет – Плевен
Индустрия	Медицински университет
Централа	Плевен, България
Площадка 1	Плевен 5800, ул. "Св. Климент Охридски" №1

2.3. За проекта

Проектът за Извършване на цялостен анализ на наличната ИТ инфраструктура в Медицински университет – Плевен е свързан с нуждата на университета да отговаря на съвременните тенденции в сигурността и защитата на информация.

2.4. Контакти

2.4.1. От страна на Възложителя

Име	инж. Христо Веселинов Маринов	Длъжност	ИТ Директор
Име	инж. Димитър Мошевски	Длъжност	ИТ Експерт
Име	инж. Илиян Милчев	Длъжност	ИТ Експерт
Име	Владислав Христов	Длъжност	Системен администратор
Име	Владислав Василев	Длъжност	Програмист

2.4.2. От страна на Изпълнителя

Име	Йордан Илиев	Длъжност	Изпълнителен директор
Е-мейл	Yordan.Iliev@MYSynergy.bg	Телефон	+359 879 166 767
Име	Младен Георгиев	Длъжност	Технически директор
Е-мейл	Mladen.Georgiev@MYSynergy.bg	Телефон	+359 889 500 080
Име	Ростислав Русinov	Длъжност	Старши ИТ консултант
Е-мейл	Rostislav.Rusinov@MYSynergy.bg	Телефон	+359 885 554 022
Име	Николай Шарков	Длъжност	ИТ консултант
Е-мейл	Nikolay.Sharkov@MYSynergy.bg	Телефон	+359 876 378 023

3. Текущо състояние

3.1. Хардуерен слой

Сървърната инфраструктура е изградена върху виртуализационен клъстер състоящ се от следните компоненти:

3.1.1. Servers

Компонент	CPU	Memory	Disk	Операционна система
Dell PowerEdge R640 server	Intel Xeon Gold 6126 CPU @ 2,60GHz	383,6 GB	223 GB	VMware ESXi 6.7.0
Dell PowerEdge R640 server	Intel Xeon Gold 6126 CPU @ 2,60GHz	383,6 GB	223 GB	VMware ESXi 6.7.0
Dell PowerEdge R640 server	Intel Xeon Gold 6126 CPU @ 2,60GHz	383,6 GB	223 GB	VMware ESXi 6.7.0

3.1.2. Дискови масиви

Компонент	CPU	Memory	Capacity	Other
Dell EMC Unity 300		48 GB	28 TB	Dual controller

3.1.3. Коммуникационно оборудване

Тип	Марка и модел	Локация	Операционна система
Маршрутизатор	Cisco ISR4351-SEC/K9	Сървърно във факултет Фармация	Cisco ISR 4300 Series IOS XE Universal Version Fuji 16.9.3
Маршрутизатор	Cisco ISR4351-SEC/K9	Сървърно във факултет Фармация	Cisco ISR 4300 Series IOS XE Universal Version Fuji 16.9.3
Защитна стена	Cisco ASA5516-FPWR-K9	Сървърно във факултет Фармация	Cisco ASA 9.8.2 Software image for ASA 5506/5508/5516 series Version 9.12.2
Защитна стена	Cisco ASA5516-FPWR-K9	Сървърно във факултет Фармация	Cisco ASA 9.8.2 Software image for ASA 5506/5508/5516 series Version 9.12.2
Layer 3 комутатор	Cisco Catalyst 3850	Сървърно във факултет Фармация	Version Everest 16.6.5
Layer 3 комутатор	Cisco Catalyst 3850	Сървърно във факултет Фармация	Version Everest 16.6.5
Комутатор	Cisco Catalyst 2960-X	Сървърно във факултет Фармация	Version 15.2.4E7
Комутатор	Cisco Catalyst 2960-X	Сървърно във факултет Фармация	Version 15.2.4E7
Комутатор	Cisco Catalyst 2960-X	Сървърно във факултет Фармация	Version 15.2.4E7
Комутатор	Cisco Catalyst 2960-X	Ректорат 1 етаж 1	Version 15.2.4E7
Комутатор	Cisco Catalyst 2960-X	Ректорат 1 етаж 1	Version 15.2.4E7
Комутатор	Cisco Catalyst 2960-X	Ректорат 1 етаж 2	Version 15.2.4E7
Комутатор	Cisco Catalyst 2960-X	Ректорат 1 етаж 2	Version 15.2.4E7
Комутатор	Cisco Catalyst 2960-X	Ректорат 1 етаж 3	Version 15.2.4E7
Комутатор	Cisco Catalyst 2960-X	Ректорат 1 етаж 3	Version 15.2.4E7

Комутатор	Cisco Catalyst 2960-X	Ректорат 1 етаж 4	Version 15.2.4E7
Комутатор	Cisco Catalyst 2960-X	Ректорат 2 етаж 2	Version 15.2.4E7
Комутатор	Cisco Catalyst 2960-X	Ректорат 2 етаж 3	Version 15.2.4E7
Комутатор	Cisco Catalyst 2960-X	Ректорат 2 етаж 4	Version 15.2.4E7
Комутатор	Cisco Catalyst 2960-X	Ректорат 3 етаж 1	Version 15.2.4E7
Комутатор	Cisco Catalyst 2960-X	-	Version 15.2.4E7
Комутатор	Cisco Catalyst 2960-X	-	Version 15.2.4E7
Комутатор	Cisco Catalyst 2960-X	-	Version 15.2.4E7
Комутатор	Cisco Catalyst 2960-X	-	Version 15.2.4E7
Комутатор	Cisco Catalyst 2960-X	-	Version 15.2.4E7
16 бр. Комутатор	Ubiquiti US-24-500W	-	Version 4.0.42
124 бр. точка за достъп	Ubiquiti UAP-AC-PRO-5	-	Version 4.0.42

Изградена е СКС на територията на Медицински университет – Плевен от тип звезда, като гръбначните трасета към етажните комуникационни шкафове за реализиране чрез оптични влакна а хоризонталните сегменти за достъп с медни проводници. СКС е категоризирана, като CAT6A.

В някои работни помещения, в които има разположени повече работни станции от наличните точки от СКС са инсталирани нисък клас мрежови устройства - неуправляеми комутатори.

Сървърното помещение е ситуирано на 4-ти етаж в сградата на факултет Фармация. Достъпът до там е със секретен ключ, който се заключва при администраторите на етажа. Изграден е двоен под а над комуникационните шкафове са подведени скари за кабелните трасета към и между тях. Комуникационните шкафове са 4, всеки с капацитет от 42 RU. Общия брой свободни RU е 77. Помещението е оборудвано със система за пожароизвестяване и пожарогасене, както и със система за прецизна климатизация. Околната среда се следи за нивото на влажност и температурата в помещението посредством Rittal CMC Monitoring system.

В първия шкаф се терминират на ODF-и гръбначните оптични влакна и точките за достъп по медни трасета на етажа, част от СКС. В шкафа са аранжирани още комутатори от старата мрежа, новата инфраструктура, контролера за точките за безжичен достъп, активно оборудване за връзка с мрежата на BREN, IP телефонна централа YEASTAR MyPBX и оборудване предоставено от доставчиците.

Втория комуникационен шкаф съдържа гръбначни комутатори, защитни стени, маршрутизатори и комутатори от периметър зоната и комутатор за управление. В него се помещава и непрекъсваемо токо-захранващо устройство (UPS).

В третия шкаф са монтирани три сървъра, които са обединени във VMware виртуален клъстер, два SAN комутатора и непрекъсваемо токо-захранващо устройство (UPS).

В четвъртия шкаф е монтиран дисковия масив и системата за мониторинг на параметрите на средата.

Безжичната мрежа е изградена посредством 124 точки за безжичен достъп. Захранването им се осъществява с PoE комутатори, свързани към Cisco комутаторите за достъп.

Счетоводството има отделна мрежа с отделен интернет, програма и сървър.

Сградата е снабдена с дизел генератор за резервно захранване. Мониторира се в Zabbix.

3.1.4. Клиенти и периферия

Не е наличен централизиран каталог на потребители и устройства. Потребителите са локални администратори за работните си станции. Придобиването на нови информационни активи (принтери, компютърни конфигурации и т.н.) не се съгласува винаги с Центъра за информационно обслужване.

Студентските потребители се създават в информационната система ЕМИС от служители на съответната канцелария. Автоматично се създава мейл и акаунт в платформата за дистанционното обучение, като се дават автоматично права. Не е ясен процеса по премахване (как потребителя става неактивен при приключване). За преподаватели, потребителите се създават от учебен отдел.

Акаунтите за служителите се създават в съответната система от собственика на системата, но не и от ЦИО. Служителите не използват служебни мобилни устройства. Няма ограничение за инсталиране на софтуер.

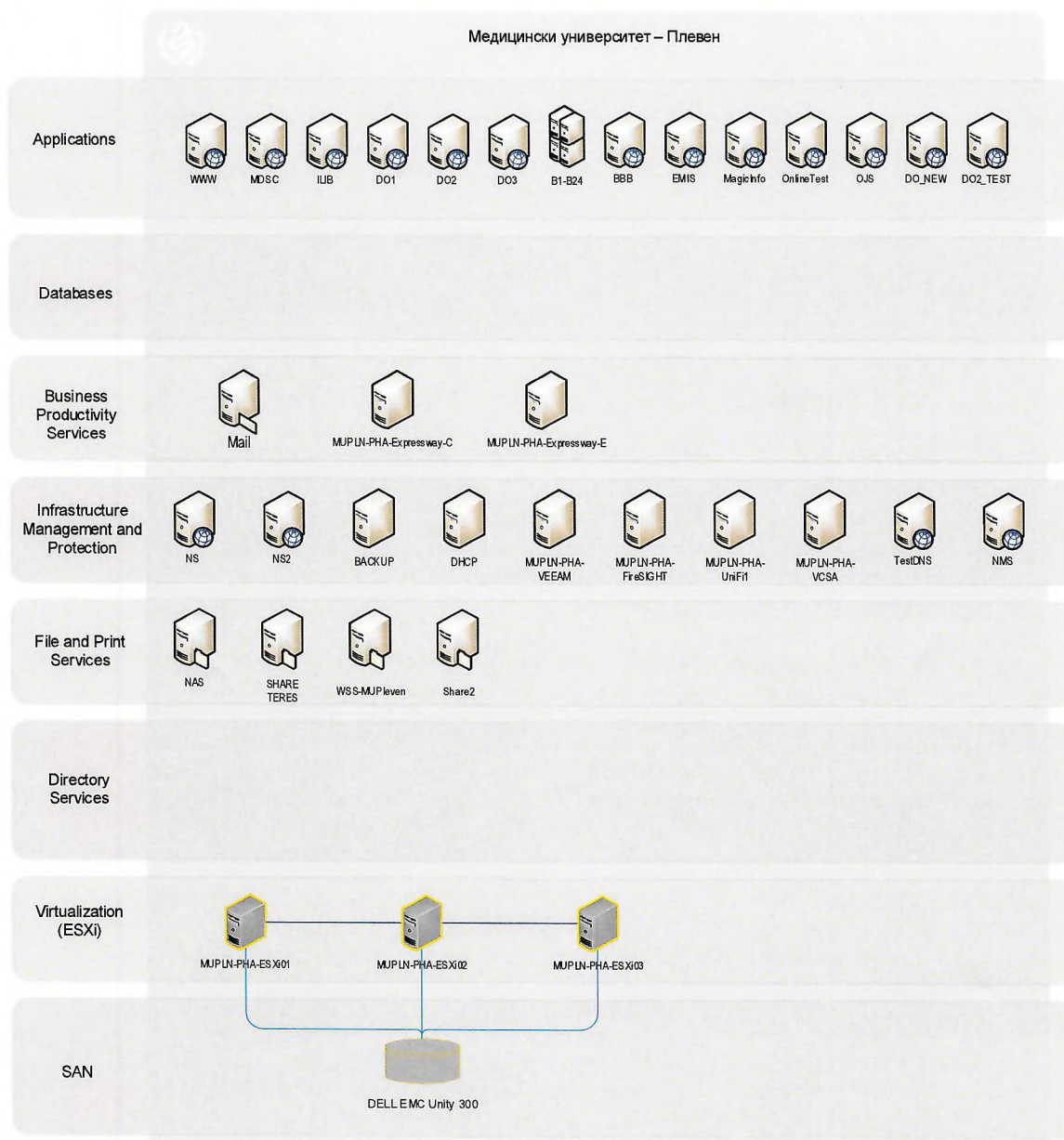
Не всички принтери са отделени в отделен VLAN. Уеб интерфейсите им за управление се достъпват без идентификация и парола. Налични са няколко принтера от висок клас. Устройствата се подменят при констатация, че устройството е старо. Обслужват се от ЦИО.

Налична е система за достъп с RFID карти но тя не обхваща всички помещения.

В сградите на кампуса са монтирани киоски за предоставяне на информация на студентите. Наличен е графика на залите и др. информация. Администрират се отдалечено с AnyDesk. Актуализират се от интернет. ОС е Windows в режим киоск с разрешение за зареждане на определени уеб страници.

3.2. Инфраструктурен софтуерен слой

На следващата фигура е представено логическото разпределение на сървърната инфраструктура:



Бележки:

- Физическите сървъри са оцветени в тъмно сиво
- Оранжева линия – сървърът е в гаранция

3.2.1. Microsoft лицензи за SaaS

Лиценз	брой
M365 A3 faculty	80
M365 A3 students	500
M365 A5 faculty	20
Office 365 A1 Plus faculty	Без ограничение
Office 365 A1 Plus students	Без ограничение

3.2.2. Електронна поща

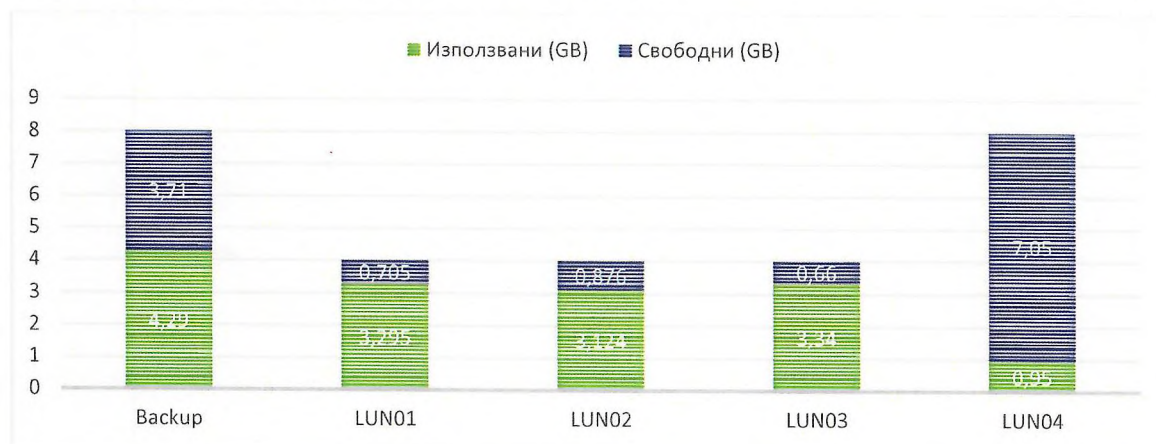
Електронна поща е инсталирана на виртуална машина с OS CentOS 7 (64-bit). Frontend-а е реализиран със свободен софтуер Roundcube. На потребителите не е разрешена функцията да сменят сами паролите си за достъп за да се ограничи възможността за различни пароли в различните системи.

Мейл клиенти на потребителите комуникират с пощенския сървър посредством не криптирани протоколи.

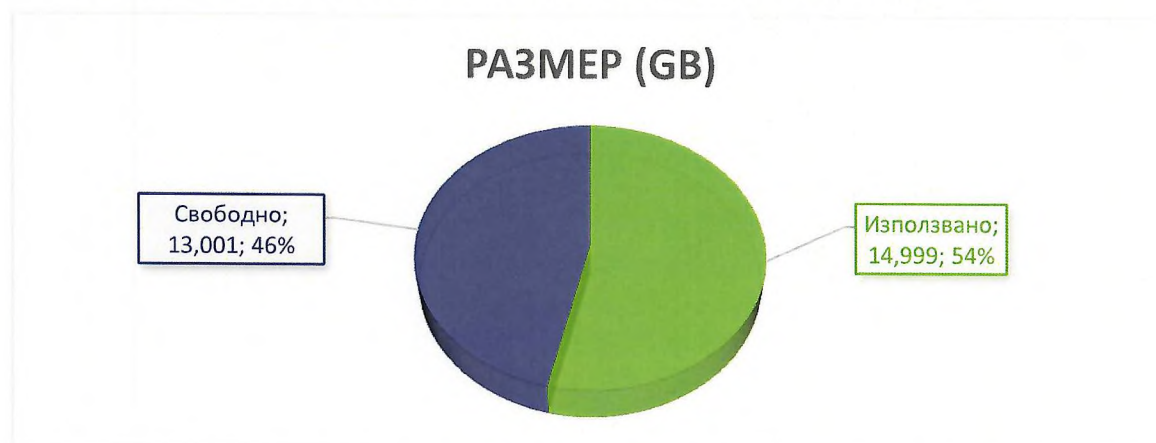
3.2.3. Файлови сървъри

Виртуалния клъстер е свързан към хранилище DELL EMC Unity 300 посредством протокол Fiber Channel през интерфейси със скорост 16 Gbps. Дисковият масив е с резервирани дискови контролери, като всеки от тях е свързан с всеки SAN комутатор с по 2 x 16 Gbps FC. Дисковото пространство е изградено от 2 tier pool съставен от Flash и SAS дисковете, като е използван и Cache pool, изграден от два диска за кеш.

Капацитета на хранилището е 28 TB разпределени в 5 LUN-а, като при три от тях свободното дисково пространство е около и под 20% от размера.



Общо дисковия масив разполага с 46 % свободно дисково пространство.



За файлови сървъри се използват виртуални машини с ОС Windows и Linux. Разположен са върху виртуален клъстер, намиращ се в сървърното помещение в сградата на факултет Фармация. Данните на 3 от 4-те определени за тази цел машини се архивират. Архивите не са резервирани на друго място и се разчита само резервираността от SAN средата. Липсва

интеграция с Активна Директория за управление на права и идентичности. Не се пазят версии на файлове за възстановяване при неволни грешки или зловредни действия за всички сървъри.

3.2.4. Активна Директория

Липсва централизиран каталог за управление на информационните активи.

3.2.5. Антивирусна защита

Няма закупен лиценз за антивирусен софтуер с централизирано управление и наблюдение. За сървърите с Linux ОС се инсталира ClamAV антивирусна защита. Някой от сървърите с ОС Windows използват вградената антивирусна защита, но не всички. Използва се Windows Defender на Windows 10 операционните системи. Някой от клиентските станции са с инсталиран NOD32 антивирусен софтуер но това е без контрола на ЦИО.

3.2.6. Биометрична идентификация

Не се използва биометрична идентификация.

3.2.7. Наблюдение на инфраструктурата

Липсва наблюдение на сървърната инфраструктурата както и сървър за събиране на събития от системите. Мрежовото оборудване се мониторира посредством конфигуриран Zabbix сървър. Налична е логическа топология на част от активното мрежово оборудване с показване на данни за натоварването на каналите и наличността на комутаторите и маршрутизаторите в реално време.

3.3. Инфраструктурен мрежови слой

В централен офис Интернет услугата се предоставя от два доставчика – Национална изследователска и образователна мрежа (посредством “Оптиспринт” ООД) и Зоната през оптична връзка. BREN - 10Gbps и 1Gbps, а Зоната – 100 Mbps. Интернет трафика се балансира между двете връзки с BREN. Връзката през Зоната се ползва ако отпадне BREN (failover).

Мрежата в централния офис е разделена в 40 VLAN-а.

VLAN	VLAN Name	Description	Network	Network restrictions	Internet access
150	Medicine	Faculty of Medicine	192.168.150.0/24	None	Yes
151	Pharmacy	Faculty of Pharmacy	192.168.151.0/24	None	Yes
152	PublicHealth	Faculty of Public Health	192.168.152.0/24	None	Yes
153	HealthCare	Faculty of Health Care	192.168.153.0/24	None	Yes
154	MedicalCollege	Medical College	192.168.154.0/24	None	Yes
155	DLST	Department of Language and Specialized Training	192.168.155.0/24	None	Yes
156	Finance	Finance	192.168.156.0/24	Private	Yes
157	Administration/ Micro	Administration	192.168.157.0/24	None	Yes
158	Printers	Printers	192.168.158.0/24	None	No
159	VideoConference	Video Conference	192.168.159.0/24	None	No
160	Library	Library Network	192.168.160.0/24	None	Yes
161	Computer-rooms	Computer rooms	192.168.161.0/24	None	Yes
162	Telec	Telec Network	192.168.162.0/24	None	Yes
163	Kiosk	Kiosk Network	192.168.163.0/24	None	Yes

164	Guest-WIFI	Guest WIFI	192.168.164.0/24	Private	Yes
165	Staff-WIFI	Staff WIFI	192.168.165.0/24	None	Yes
166	Student-WIFI	Student WIFI	192.168.166.0/24	Private	Yes
167	IPCAM	IP cameras only	192.168.167.0/24	None	No
168	APNetwork	AP management network	192.168.168.0/24	None	Yes
169	Management	Management Network	192.168.169.0/24	None	Yes
170	Core-ASA	Infrastructure VLAN from core switch to ASA	192.168.170.0/27	None	No
270	ASA-Router	Infrastructure VLAN from ASA to routers	192.168.170.32/27	None	No
172	Servers-DMZ	Servers - DMZ	192.168.172.0/24	None	No
173	VMware-MGMT	VMware MGMT	192.168.173.0/26	None	Yes
174	VMware-vMotion	VMware - VMware vMotion	192.168.173.64/26	None	No
175	VMware-FT	VMware - Fault Tolerance	192.168.173.128/26	None	No
176	VMware-Reserved	Reserved	192.168.173.192/26	None	No
178	AccessControl	Access Control Network	192.168.175.0/24	None	No
179	BridgeVLAN	VLAN for Mikrotik	192.168.176.0/24	None	No
181	Servers-Data	Servers - Data	192.168.177.0/24	None	No
180	IPT	IP phones	192.168.0.0/24	None	Yes
190	Mikrotik	Old network	194.141.67.0/24	N/A	N/A
195	Backup-ISP	Zonata	85.217.195.192/26	N/A	N/A
250	BREN-Primary	BREN-Primary	194.141.253.144/30	N/A	N/A
251	BREN-Backup	BREN-Backup	194.141.252.144/30	N/A	N/A
555	NATIVE	Native vlan	N/A	N/A	N/A
N/A	N/A	VPN pool	192.168.180.0/24	None	Yes
145	Conference-systems	Conference systems	172.16.250.0/24	Private	No
146	VR360	VR360	172.16.251.0/24	Private	No
149	Knijarnica-PHA	Knijarnica-PHA	192.168.149.0/24	Private	Yes
513	Dormitory	Infrastructure VLAN to dormitory	172.16.100.0/24	None	Yes

Комуникационната инфраструктура е разделена на отделни сегменти на база предназначението и функционалността, която ще изпълнява всеки един от тях. В текущия дизайн са реализирани следните сегменти:

Периметър зона – осъществява връзка към външни комуникационни инфраструктури. В нея са включени резервирана двойка периметър комутатори от серията Cisco 2960-X, резервирана двойка маршрутизатори Cisco ISR 4351, както и резервирана двойка защитни стени Cisco ASA 5516 с FirePower функционалност, която осигурява контрол на приложения, инспектира клиентския трафик за разпознаване, неутрализиране, превенция на атаки и заплахи (IPS), осигурява защита от зловреден софтуер, както и осигурява функционалност за филтриране на URL адреси базирано на репутация и категории. Тези устройства осигуряват високи нива на

информационна сигурност, както и надеждност на връзките в допълнение на високата отказоустойчивост на реализирания дизайн на периметър зоната.

Гръбнак на мрежата – изграден от комутатори Cisco Catalyst 3850. Осигуряват надеждна и високоскоростна Layer 3 връзка между всички мрежови сегменти – периметър, сегмент за достъп и сървърната инфраструктура.

Сегмент за достъп – сегментът се състои от комутатори от серията Cisco 2960-X, които са свързани към опорните комутатори Cisco Catalyst 3850 посредством 2 броя 10Gbps SMF оптични връзки. Сумарния капацитет между сегмента за достъп и гръбнака на мрежата е 20Gbps.

Комутатор за управление – комутатор от серията Cisco 2960-X реализира независима мрежа за управление от типа OOB (Out of Band). Обединява всички портове за управление от периметър устройствата, опорните комутатори, сървърите и устройствата за съхранение на данни.

Безжична комуникация – посредством 124 броя безжични точки за достъп от серията Ubiquity UAP-AC-PRO, захранени от Ubiquity US-24-500W комутатори поддържащи Power over Ethernet (PoE+) съгласно стандарти 802.3af и 802.3at. Към 12 от точките към момента няма връзка. Комутаторите са свързани посредством 1 брой 1Gbps медна връзка към сегмента за достъп. UniFi Controller е инсталиран на виртуална машина (MUPLN-PHA-UniFi1) в клъстъра. Софтуерът се използва за централизирано и автоматизирано управление на точките за достъп. Системата излъчва 3 мрежи в ефира – за гости, студенти и персонал. Паролите за трите SSID са статични и не се сменят периодично във времето.

В сградата на факултет Фармация телефонията се осъществява с VoIP централа YEASTAR MyPBX. 20 телефона се използват от тази централа. В останалите сгради се използва стара телефонна централа с над 200 телефонни поста.

Камерите за видео наблюдение са достъпни от Интернет чрез отворени портове на защитната стена.

3.4. Приложен софтуер

3.4.1. HR и счетоводен софтуер

За счетоводен софтуер се използва Конто. Той е разгърнат в отделна мрежа на сървър извън сървърното помещение, която ползва отделна Интернет връзка.

За нуждите на човешки ресурси и TPЗ се използва софтуер TERES. Софтуера използват файлов сървър Share (WIN-M1T01GTSVFT) за съхранение на базите си от данни. ОС е Microsoft Windows Server 2016 Datacenter.

3.4.2. Деловодна система

Деловодната система е инсталирана локално на компютърна станция. Води регистър на деловоден номер и заглавие на документа, но не съхранява дигитализирани копия на документа. Няма информация да се правят резервни копия извън локалната машина.

3.4.3. Информационна система за управление на образованието

Основната информационна система в университета ЕМИС е разгърната върху emis.mu-pleven.bg с ОС CentOS 7. За тази версия на ОС предлагането на пълни актуализации от производителя е приключило преди повече от година а актуализациите за поддръжка и сигурност ще приключат през юни 2024 г.

Софтуерът ЕМИС е разработен с език за програмиране PHP, а backend-а на системата се реализира с MySQL. Разделен е на следните потребителски модули:

- ADMIN – Регистър на студенти и преподаватели;
- COMMON – Обобщени функции;
- FOREIGN – Чуждестранни студенти;
- KSK – Кандидатстудентския модул;
- SPRAVKI – Справки в обобщени функции;
- ANKETA – Управление на атестационни карти;
- EVRO – Център за ежроинтеграция;
- foreignnsk – Кандидатстудентски модул чуждестранни студенти;
- KSKBUR – Кандидат-студентския модул;
- USER – Използване без администраторски права;
- CAREER – Кариерен център;
- EXPERT – Управление на учебния процес;
- GRADU – Управление на специализанти;
- LIBRARY – Библиотека;
- SEDO – Система за електронно и дистанционно обучение;
- FINANCE – Финансова дирекция;
- HR – Човешки ресурси;
- NID – Акредитация и атестация;
- WEBSYS – WEB/SYS Admins.

Информационната система съхранява сканирани копия на издадените от университета дипломи. Плащанията онлайн се извършват през виртуален POS терминал. При плащане на място се въвеждат от служителите на ЦИО в системата ръчно извършените транзакции.

Модула за класиране на кандидат-студенти е сложен и разработчика не желае да го развива или поддържа. Самия процес е комплициран и текущата разработка генерира грешки при кампания за класиране.

Наличен е сключен договор за поддръжка на платформата. Липсва специфицирано ниво на обслужване на системата от доставчика и описание задълженията на доставчика.

3.4.4. Дистанционно обучение

Използваната платформа за дистанционно обучение е moodle. Съдържа информация за всички факултети, специалности и предмети. Интегрирана е с Big Blue Button за провеждане на онлайн занятия.

Платформата за дистанционно обучение е разгърната на do2.mu-pleven.bg. Машината do3.mu-pleven.bg разпределя видео потока от Big Blue Button към 24 Vx машини за виртуални класни стаи. Не се използва интеграция с Microsoft Teams.

На onlinetest.mu-pleven.bg е публикувана moodle платформа за онлайн тестове и курсове за кандидат-студенти. bbb.mu-pleven.bg се използва за връзка с onlinetest.

На do1.mu-pleven.bg се намира стара използвана версия на moodle с Big Blue Button.

Наличен е сключен договор за поддръжка на платформата.

3.4.5. Библиотечен каталог

Разработената система използва PHP и Microsoft Access, като backend. Файловете се пазят на файлов сървър. Служителите на библиотеката управляват съдържанието през Microsoft Access а потребителите го достъпват през уеб интерфейс.

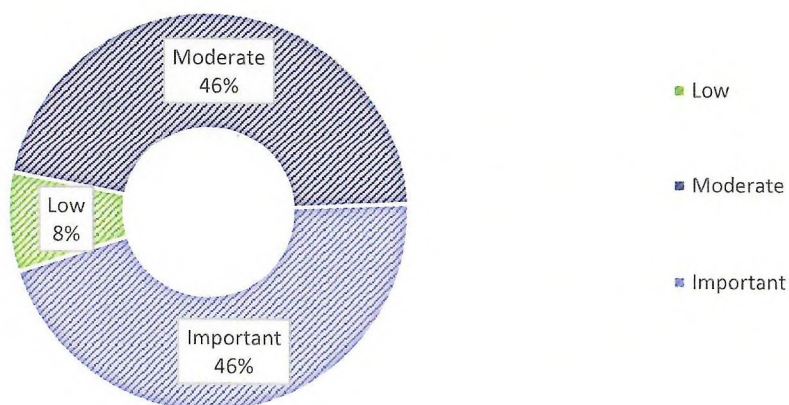
Системата е разгърната върху ilib.mu-pleven.bg (WIN-G3DO6RKG9CC) и WSS-MUPleven за файлово хранилище. ОС на машините е Microsoft Windows Server 2008 R2, чиято поддръжка от производителя е приключила преди повече от година.

3.5. Сигурност

Не са налични разписани процеси по управление на сигурността и защита на информацията. Липсва Активна Директория а от там и не са налични конфигурирани централизирани политики за защита на устройствата. Налице са споделени пароли за администриране, които се съхраняват некриптирани и в явен вид. Липсва разделяне на правата на потребителите. Работните компютри не се управляват през Активна Директория. Реализирано е сегментиране на мрежите на логическо ниво, но не са документирани правила за ограничаване на комуникацията между отделните сегменти. Липсва антивирусен софтуер с централизирано наблюдение. Пощенския сървър не позволява адекватно ниво на защита от вируси и спам.

Налични са сървъри с ОС извън поддръжка от производителя. Липсват критични актуализации. Подробна извадка по сървъри и липсващи актуализации е налична в Приложение 2 към доклад. В одитираната извадка виртуални машини от липсващите актуализации, приблизително половината са с високо ниво на тежест (severity), както е видно на следващата графика.

Липсващи актуализации



Бизнес приложенията използвани от университета не покриват регулаторните изисквания за информационна сигурност, поради архитектурни лимитации на самите софтуери. Част от несъответствията са свързани с невъзможност да бъдат разделени на физическо или логическо ниво, като уеб сървърът, сървърът с приложния софтуер и сървърът с базата данни на една

информационна система трябва да са разположени на различни машини и в различни мрежи. Част от системите не използват СУБД, което повишава риска от компрометиране на данните.

Поради широката гама от услуги и информационни активи на университета, наличният екип от 5 служители на ЦИО, не е в състояние да обезпечи администрирането на всички системи, да осигури разделение ролята на администраторите, както и да осигури заменяемост за всяка от ролята. В допълнение, липсва адекватен капацитет за третиране на инциденти с висока критичност и/или обхват.

3.6. Непрекъсваемост на системите

3.6.1. Резервираност на сървъри и приложения

Сървърната инфраструктура е резервирана чрез виртуализационен клъстер, състоящ се от три сървъра и използва платформа VMware vSphere 6. Сървърите са свързани чрез Fibre Channel протокол до дисков масив Dell EMC Unity 300, използвайки два Cisco MDS 9148S 16G Multilayer Fabric Switch-a. Използват се два контролера на дисковия масив, два комутатора и по две FC порта на HBA към всеки от трите сървъра, което гарантира непрекъсваемост на връзките.

Връзката между двата опорни комутатора и сървърите е реализирана посредством 2 интерфейса към всеки със скорост на пренос 10Gbps за всеки от сървърите. Резервираността на връзките се осъществява на ниво хипервайзор (VMWare). Портовете от страна на опорните комутатори са конфигурирани в режим „трънк“.

Всяко от звената на клъстера разполага с капацитет от 383,6 GB оперативна памет.

Сървърите са с локални административни потребители. Няма реализирана резервираност на ниво операционна система или на ниво приложение за някои от сървърите и приложенията на организацията.

Няма реализирана резервираност на данните и/или виртуалната инфраструктура във втори център за данни.

3.6.2. Резервираност на мрежа

За осигуряване на комуникациите в Интернет периметъра се използват резервирана двойка периметър комутатори от серията Cisco 2960X, резервирана двойка маршрутизатори Cisco ISR 4351, както и резервирана двойка защитни стени Cisco ASA 5516 с FirePower функционалност. Периметър комутаторите Cisco 2960-X са обединени в една логическа система, използвайки Cisco технологията – FlexStack+ чрез стекиращ кабел.

Вътрешната мрежа се маршрутизира от два Layer 3 опорни комутатора Cisco 3850 обединени в една логическа система, използвайки Cisco технологията – StackWise-480 чрез специален за целта стекиращ кабел. Чрез използването на SVI интерфейси при отпадане на един от двата опорни комутатора, Layer 3 интерфейса не отпада, а продължава да работи на другия комутатор.

EtherChannel се използва за връзките между комутаторите за достъп и опорните комутатори, както и между опорните комутатори и комутатора за управление. В локалната мрежа се използва Rapid PVST+, който представлява отделно копие на RSTP във всеки VLAN.

3.6.3. Архивиране на системите

Софтуерът за извършване на архивни копия, е базиран на специализирания продукт за защита на виртуална среда – Veeam Backup & Replication Enterprise - Education Sector, който има следните основни функционалности:

- Защита на цяла виртуална машина;
- Моментално възстановяване чрез използване директно на бекъп файла;
- Възстановяване на отделни файлови обекти във виртуалната машина;
- Лимитирано възстановяване на отделни обекти от конкретни приложения и бази данни;
- Вградени методи за дедупликация и компресия на данните;
- Репликация на защитените данни на отдалечена инфраструктура;

Налични са бекъп планове за архивиране. Конфигурирани са автоматизирани бекъпи за приблизително 60% от виртуалните машини. Не се извършват процедури по тестово възстановяване на данни. Няма разписан план за възстановяване на системите при аварии. Няма оценка на критичността на системите и бизнес нуждите за RTO и RPO. Архиви не се изнасят на втора локация.

Бекъпите на системата ЕМИС се пазят на отделен сървър извън плановите на Veeam. Самата машина се бекъпира в плановите на Veeam.

4. Констатации по текущото състояние

За оценката на риска на всяка от констатациите е използвана следната категоризация с цел определяне на въздействието върху дейността на организацията:

Ниво	Въздействие върху непрекъснатост на дейността
Несъществено - 1	Тези рискове имат несъществено въздействие, не водят до нарушаване на нормативно, регулаторно или договорно изискване, прекъсване на процеси/услуги или забавяне на текущата дейност.
Ниско - 2	Рисковете с ниско въздействие не водят до нарушаване на нормативно, регулаторно или договорно изискване, и до прекъсване на критични процеси/услуги. Могат да доведат до краткотрайно нарушаване на достъп до ИКТ или загуба на информация, които са незначителни или могат да бъдат възстановени в най-кратки срокове.
Средно - 3	Рисковете със средно въздействие, обикновено са за кратък период и са контролируеми. С правилните защити и противодействие, въздействието им може да бъде намалено до незначителни затруднения и минимални загуби. Рисковете със средно въздействие могат да доведат до несъществено нарушаване на договорно изискване или до нарушаване на достъп и загуба на информация. Не водят до нарушаване на нормативни и регулаторни изисквания. Могат да доведат до прекъсване на некритични процеси/услуги.
Високо - 4	Рисковете, с високо въздействие, водят до средни финансови загуби и до намаляване на общественото доверие. Могат да доведат до значително нарушаване на договорно изискване или до нарушаване на конфиденциалността, достъп и загуба на информация, които могат да бъдат възстановени със значителни загуби. Могат да доведат до нарушаване на нормативни и регулаторни изисквания. Могат да доведат до прекъсване на критични процеси/услуги.
Много високо - 5	Рисковете с много високо въздействие, могат да бъдат унищожителни, ако незабавно не се приложи подходящо противодействие. Характеризират се със значителни потенциални финансови загуби, съществени санкции и загуби от неспазване на нормативни, регулаторни или договорни изисквания, загуба на общественото доверие или невъзможност да се възстанови критичен процес или услуга.

	Риските с много високо въздействие могат да доведат до прекъсване на критично важни процеси/услуги и/или до нарушаване на конфиденциалността, достъпа и загуба на критични ИКТ и бази-данни, които могат да бъдат възстановени със съществени разходи/загуби.
--	---

При наличие на риск с голям обхват върху инфраструктурата, то неговото ниво се повишава.

В следващата таблица са описани констатации на базата на направения одит. За всяка от констатациите е определено ниво на въздействие върху дейността на организацията.

№	Констатации	Ниво
K01	Липсва репликация на виртуални машини във втори център за данни	3
K02	Липса на разпределена архитектура на услугите – наблюдава се смесване на приложния софтуер с бази данни и инфраструктурни услуги, което понижава сигурността и устойчивостта на системите и може да доведе до загуба на информация, компрометиране или отпадане на система	4
K03	Възможност за по-ефективно използване на наличните софтуерни SaaS лицензи	1
K04	Липсващи възможности, средства и процеси по отношение на политики за защита на устройства и потребители	4
K05	Не се използва Tier Model в администрирането – не е реализирано разделение на ролята и администрирането на системите	3
K6	Липсва история на версиите и защита от крипто вируси и други заплахи на файловия сървър	4
K7	Липсва сървър за управление на печата и наблюдение на принтери – използването на централен сървър улеснява значително администрирането на услугата по печат и повишава нейното качество	2
K8	Липсващи възможности, средства и процеси по отношение на политики за управление на компютърни станции и сървъри	4
K9	Архиви – липсва архивиране на отдалечена локация	4
K10	План за непрекъсваемост – липсва категоризация на услугите, определено RTO и RPO, имплементация и контрол на процеса	4
K11	Липсващи възможности, средства и процеси по отношение на управление на сигурността – липса на централизирана антивирусна защита за работни станции и сървъри, липса на система за събиране и обработка на събитията и не се изпълнява периодично сканиране за уязвимости в системите	4
K12	Ограничени пощенски кутии от към възможности – използва се нисък клас пощенска услуга с ограничено пространство, функционалности и ниско ниво на сигурност и контрол, както и липса на интеграция с останалите системи и услуги.	3
K13	Пощенската услуга не предоставя възможност за синхронизация на календари, контакти и други	1
K14	Използват се традиционни средства за съвместна работа – производителността и възможностите на служителите за колаборация помежду им са силно ограничени	2
K15	Софтуерът на част от сървърите и устройствата не се обновяват регулярно или никога не е обновяван. Приложение 2	4
K16	Съществуват неуправляеми комутатори в мрежата	2
K17	Липса на централизиран и автоматизиран модел на администриране – висок риск от компрометиране на ИТ средата	3
K18	Ограничени възможности за защита на ИТ инфраструктурата – липса на мониторинг на сървъри, приложения и услуги, процес за управление на	4

	уязвимостите, план за реакция при инциденти, не се регистрират административните действия	
K19	Достъп до безжична мрежа – вписването в безжичната мрежа не използва роуминг идентификация, статични пароли уязвими към компрометиране	4
K20	Липса на централизиран каталог – управлението на потребители, клиентски устройства и сървъри без наличие на Активна Директория възпрепятства прилагането на единна и хомогенна политика за сигурност, както и ограничава видимостта върху активите и ресурсите	5
K21	Система за управление на пароли – липсва система за съхранение на пароли в криптиран вид с управление на достъпа до записите	5
K22	Защита на уеб сървъри – липсва покриването на регулаторни изисквания към headers на отговорите на заявки за уеб сайтове, на част от сървърите са публикувани приложения без автоматично пренасочване към канал през криптиран протокол	4
K23	Процедури или инструменти, контролиращи инсталирането на софтуер – потребителите са администратори на компютрите си, липсва контрол на инсталирания софтуер и инвентаризация	4
K24	Доставчика на основната информационна система за управление на образованието ЕМИС няма гарантирани нива на услугата	4
K25	Наличният състав на ЦИО не може да осигури обезпечаване работата на широката гама от налични информационни активи	4
K26	Отделната мрежа на счетоводството повишава риска от компрометиране	4
K27	Налични са сървърни ОС с приключила поддръжка от производителя – сървърите обезпечават услуги на библиотеката са с версия на ОС 2008	4
K28	Бизнес приложенията обезпечават процесите на университетската администрация не покриват регулаторни изисквания за информационна сигурност	4

5. Визия и препоръки

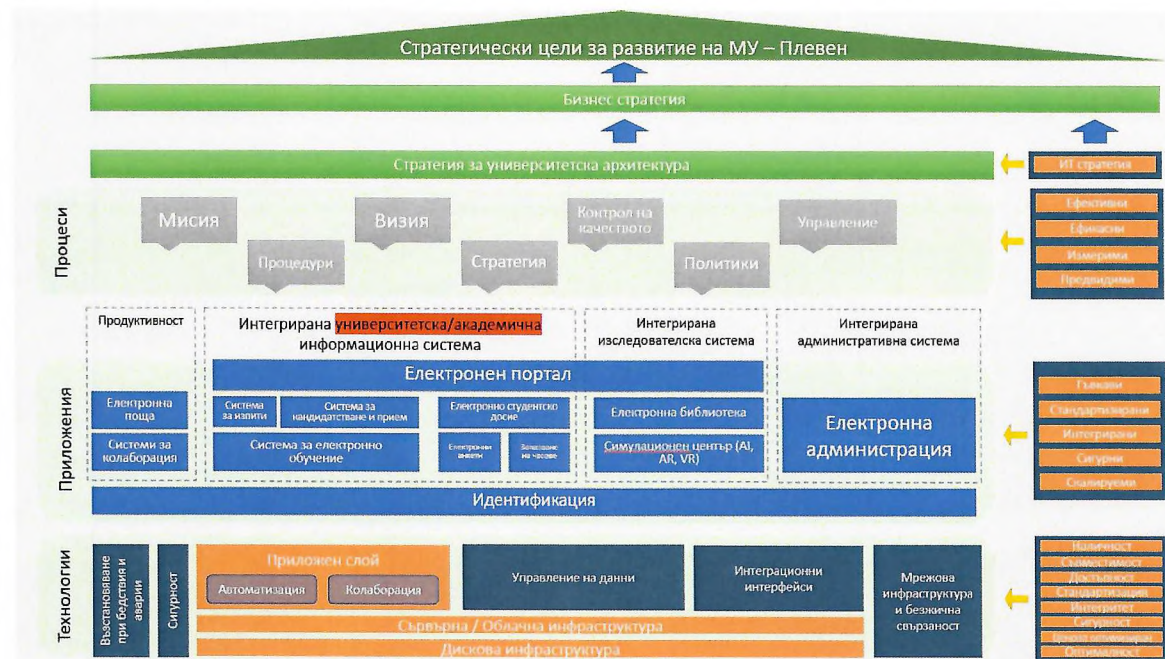
5.1. Визия



5.2. Дизайн

В следващите таблици е съпоставено текущото състояние, проблемите и ограниченията и е предложен бъдещ дизайн съобразен с добрите практики в изграждането на мрежи и информационни системи. Дизайнът е съобразен с текущия хардуер и софтуер на организацията, като максимално се използват наличните ресурси. Продуктите и услугите на Майкрософт са предложени в бъдещия дизайн, тъй като разширяват и надграждат вече наличните лицензи от същия производител.

Дизайнът е съобразен и със стратегическите цели за развитие на МУ Плевен:



5.2.1. Ограничения и зависимости при изпълнение на дизайн

ИД	Категория	Ограничение/зависимост
CD01	Информационен център	Планирано закупуване на втори дисков масив и допълнителни два хоста
CD02	Инфраструктурна сигурност	Изискване за интеграция с eduGAIN федерация за идентичности
CD03	Възстановяване при бедствия и аварии	Липса на възможност за бързо възстановяване на услугите при авария на ИЦ в отдалечен ИЦ Липса на възможност за изнесено съхранение на архивни данни от системите
CD04	Приложения	Част от бизнес приложенията са с ограничена архитектура, която не може да покрие съвременните стандарти.
CD05	Софтуер	Липсва лиценз за централизирана антивирусна система

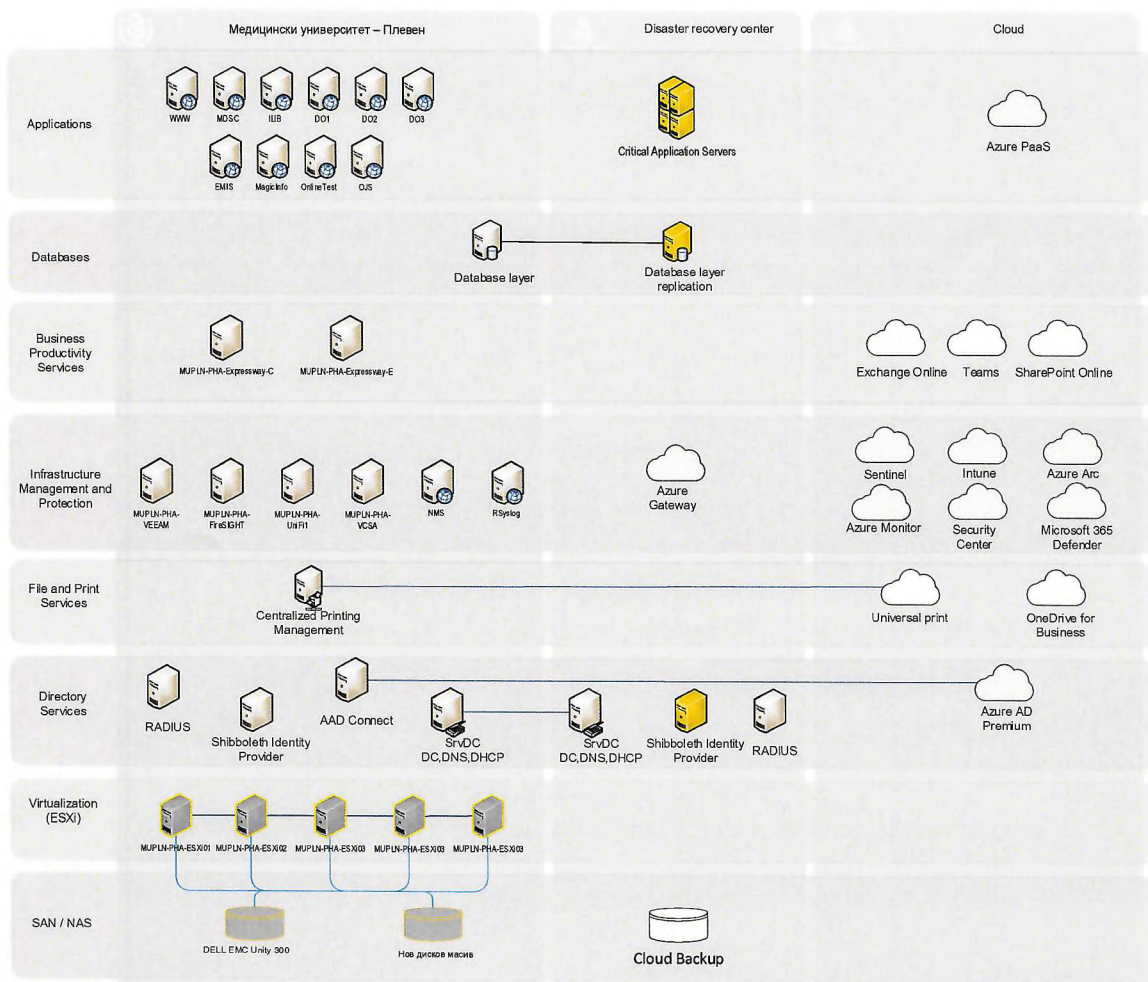
5.2.2. Дизайн на високо ниво

Услуга	Текущо състояние	Проблеми, ограничения	Бъдещо състояние	Бележки
Server Virtualization	- Клъстер от 3 сървъра 54 виртуални машини на клъстера - Резервирана връзка към SAN - Сървърите и дисковите масиви са в гаранция	Съществуват услуги на сървъри извън клъстера	100% от продукционните виртуални машини са резервирани върху клъстер	
Active Directory	- Липсва Активна директория - DHCP – липсва резервираност	- Усложнение в администрирането поради липсата на Активна Директория - Липсват разработени политики за защита на устройства и потребители - Не се използва Tier Model за администриране	- Централизирана топология – AD, DNS, DHCP - Реализиран Tier модел - Висока наличност на централизирана услуга за управление на идентичности - Защита на идентичностите с Azure AD	В бъдеще е възможно създаването на „bastion forest“ за администриране

		•Различни идентичности в системите за потребителите намалява нивото на сигурност	•Използване на Azure AD SSO от приложенията •Възможност за интеграция с глобална федерация за идентичности eduGAIN	
File and Print Services	•Файловите услуги се предоставят чрез няколко сървъра като един от тях е с ОС Windows Server 2008 •Липсва сървър за управление на печат	•ОС без поддръжка от производителя •Липсва интеграция с Активна Директория •Липсва история на версиите и защита от крипто вируси и други заплахи •Трудна достъпност на файловата услуга отдалечено •Липсва сървър за управление и наблюдение на печата	•OneDrive for Business с интеграция с Активна Директория •Синхронизация на файлове с локално копие на потребителските компютри •Архивиране на всички потребителски профили •Централизиран сървър за управление на печата	•Използват се вече закупените лицензи на Майкрософт
Infrastructure Management	•Липсва централизирано управление на устройства •Липсва централизирано управление на сървъри •Виртуалната инфраструктура се управлява централизирано чрез vSphere •Използват се киоск устройства в публичните пространства	•Липсват политики за управление и защита на устройства •Липсващи възможности, средства и процеси по отношение на управление на сигурността	•Intune – управление на компютри, киоск и мобилни устройства навсякъде; управление на служебната информация при BYOD •Azure Arc – управление на хибридна сървърна инфраструктура Windows и Linux	•Използват се вече закупените лицензи на Майкрософт Intune
Infrastructure Protection	•Налична е висок клас NGF •Мрежовата инфраструктура се наблюдава чрез Zabbix •Липсва централизирана антивирусна за компютри и сървъри	•Няма обособен втори ИЦ •Липсва централизирано управление и анализ на събитията (SIEM), както и защита от подправяне на историята на действията •Липсва Security Monitoring, Vulnerability Management за сървърната и софтуерна инфраструктура •Липсва архивиране на отдалечена локация •Няма резервираност на критичните услуги във втори ИЦ	•Репликация на критични услуги в резервен център •Анализиране на събития – Azure Monitor, Sentinel •Защита за сървъри – Azure Security Center •Защита за работни станции – Microsoft 365 Defender	
Business Productivity Services	•Използва се пощенска услуга, с ограничени бизнес възможности и защита •Няма лесна възможност за колаборация и обмяна на файлове при работа по проекти •Използва се Big Blue Button софтуер с интеграция с moodle	•Ограничени пощенски кутии •Паролите не могат да се сменят •Липсва синхронизация на календари, контакти и други •Използване на традиционни средства за съвместна работа •Ниско ниво на сигурност на пощенската услуга •Ниско ниво на сигурност на Big Blue Button, поради архитектурата на системата •Big Blue Button консумира високо количество ресурси, усложнява администрирането и създава рискове за мрежовата сигурност	•Дългосрочно всички услуги се предоставят от Microsoft 365 •Exchange Online •Въвеждане на модерен подход за колаборация •Контрол върху информацията и защита от изтичането ѝ •Teams/SharePoint услуга за колаборация и обмен на файлове •Teams SaaS за лесна администрация и скалируемост •Интеграция на Teams и moodle	•Използват се вече закупените лицензи за Microsoft 365
Network	•Два доставчика на Интернет •Налична защитна стена NGF •Сдвоени опорни комутатори за L3 рутиране на вътрешната мрежа	•Липсва на разписани правила за ограничение на трафика между вътрешните мрежи •Остарели устройства извън поддръжка	•Документиране и контрол ограниченията на трафика между сегментите на мрежата •Интегриране с бъдещи идентификатори от	

•Сегментиране на логическо ниво •Централизирано и автоматизирано управление на точките за достъп •Наличие на неуправляеми устройства	•Паролите за трите WiFi SSID са статични и не се сменят периодично във времето •Правата за достъп до излъчваните мрежи не са индивидуални	•централен каталог, RADIUS, eduroam и т.н. •Индивидуално удостоверяване на принципа SSO	
--	--	--	--

5.2.3. Дизайн на сървърна инфраструктура

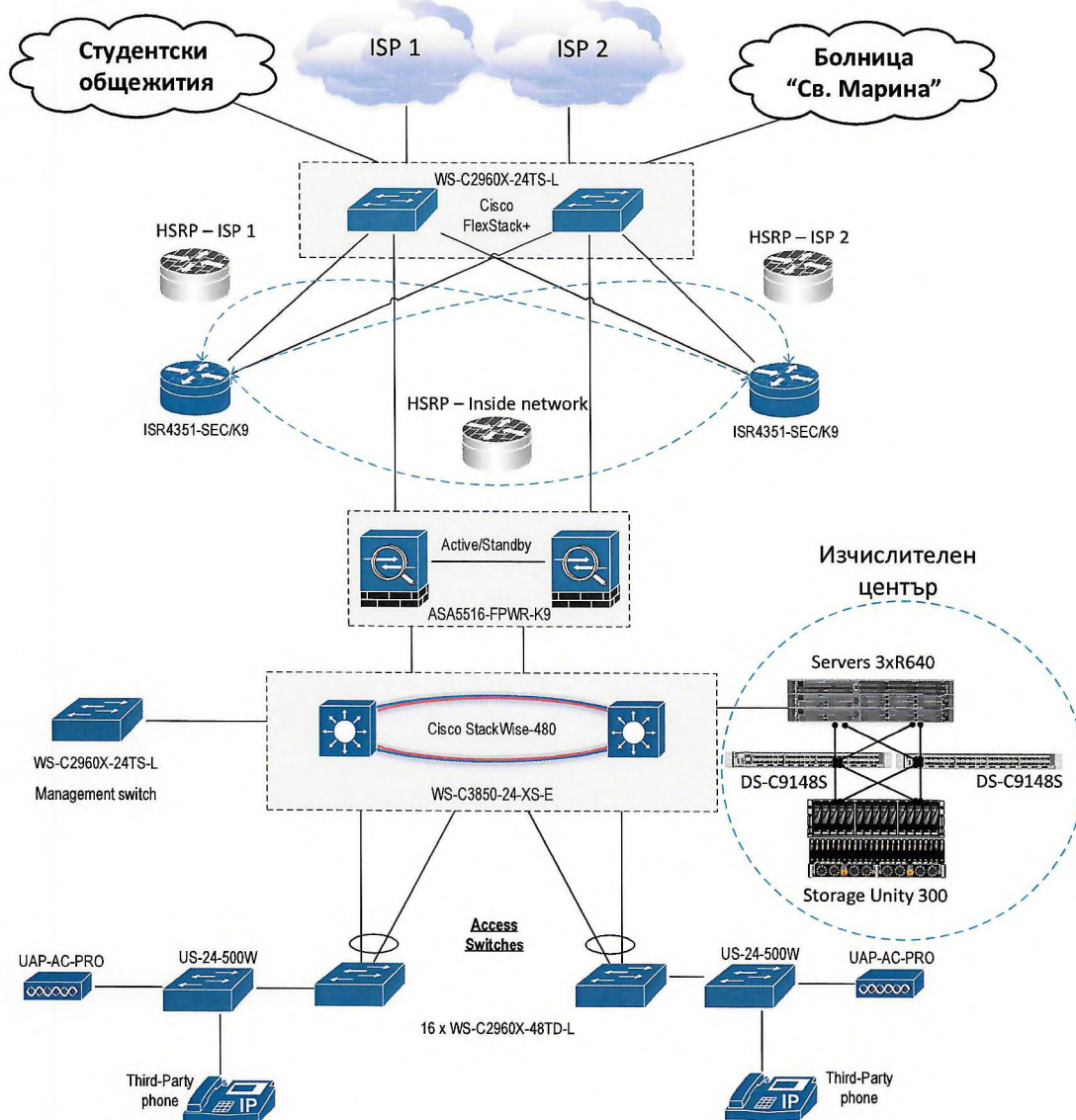


Бележки:

- Физическите сървъри са оцветени в тъмно сиво
- Реплики на виртуални машини са оцветени в оранжево
- Оранжева линия – свързания хардуер е в гаранция

5.2.4. Дизайн на мрежова инфраструктура

Мрежовата инфраструктура е резервирана, а топологията е с високо ниво на отказоустойчивост.



5.3. Инициативи

В таблицата са представени дейностите за постигане на целевия дизайн на инфраструктурата:

№	Проект	Описание	Необходим ресурс
1	Модернизация и оптимизация на ИТ инфраструктурата		
1.1	Изграждане на Майкрософт Активна Директория и Azure AD	Разгръщане на Майкрософт Активна Директория, конфигурация на организационна структура, политики, DNS, DHCP, сайтове, инсталация на домейн контролери. Конфигуриране на синхронизация с Azure AD и политики за сигурност от Azure.	Сървърен ресурс за 2 домейн контролера. (наличен) Microsoft 365 лицензи (наличен)
1.2	Виртуализиране на хардуерни сървъри	Преместване на счетоводния сървър върху виртуализационния клъстер. Разгръщане на Windows	Сървърен ресурс за приложните сървъри и backend-a. Лицензи за Azure.

		Virtual Desktop за преместване на софтуерните продукти като деловодната система и др.	
1.3	Внедряване на Identity Provider за eduGAIN	Планиране и внедряване на услуга за идентификация с Shibboleth Identity Provider. Инсталиране на виртуална/и машина/и за осигуряване на услугата.	Сървърен ресурс за виртуалните машини. (наличен)
1.4	Модернизация на файловата услуга	Присъединяване на файловия сървър към новоизградения домейн. Конфигуриране на споделени ресурси, и миграция на съдържание. Разгръщане на DFS и конфигурация на репликация.	Сървърен ресурс за виртуалните машини. (наличен)
1.5	Внедряване на RADIUS AAA	Планиране и внедряване на услуга за идентификация на потребителите. Преконфигуриране на UniFi контролера. Преконфигуриране на мрежовото оборудване за работа с единна идентификация.	Сървърен и дисков ресурс за управление заявките за идентификация. (наличен)
2	Повишаване на производителността на потребителите		
2.1	Миграция към Exchange Online	Миграция на съществуващата пощенска услуга към Exchange и конфигурация на календари, споделени кутии, управление на зали и други	Microsoft 365 лицензи (наличен)
2.2	Миграция към SharePoint и OneDrive for Business	Миграция на съществуващ файлов сървър към SharePoint и реализация на архив на компютърни станции в OneDrive for Business.	Microsoft 365 лицензи (наличен)
2.3	Модернизация на административни процеси	Внедряване на система за управление на административни процеси (деловодство, заявки за отпуск, заявки за консуматив и други)	Сървърен и дисков ресурс (наличен) Лиценз за софтуер
2.4	Внедряване на управляем печат	Консолидация и обновяване на устройствата за печат както и въвеждане на централизирано управление и контрол на печата	Наемане или закупуване на устройства за печат Лицензи за централизиран печат
2.5	Внедряване на Teams и интеграция с moodle	Настройка и организация на работни области според спецификата на клиента. Конфигуриране на moodle за работа с Teams.	Microsoft 365 лицензи (наличен)
2.6	Внедряване на SIS	Внедряване на SIS система. Анализ на бизнес процесите. Настройки, адаптиране и конфигуриране на средата. Миграция на данни.	Бизнес консултанти за разписване на проект Лицензи за софтуер Сървърен и дисков ресурс или IaaS (наличен)
3	Подобряване на информационната сигурност		
3.1	Внедряване Azure Security – идентичности, сървъри и компютри	Конфигурация на Azure Active Directory политики за сигурност, Azure Monitor, Sentinel, Security Center, Azure Arc и Microsoft 365 Defender	Лицензи за Azure
3.2	Внедряване на хибриден облак с репликация	Конфигурация на архивиране на втора локация. Конфигуриране на репликация на критичните виртуални машини.	Лицензи за Azure
3.3	Защита на работните станции	Конфигурация на политика за управление и защита на работни станции	Microsoft 365 лицензи (наличен)
3.4	Внедряване на Tier модел	Създаване на стратегия и дизайн на високо ниво за разделение на средата и администрирането.	-
3.5	LAPS	Внедряване на система за уникални пароли на компютърни станции и сървъри	-
3.6	Редизайн на сегрегирани мрежи и трафика между тях	Анализ и дефиниране на трафика между събнетите. Конфигуриране на правила спрямо новата домейн архитектура.	-
3.7	Внедряване на СУСИ, съобразно ISO 27001:2017	Разработване на политики за информационна сигурност.	-

5.4. Пътна карта

Изготвената пътна карта е препоръчително разпределение на проектите в срок до 3 години. Разпределението е съобразено със зависимостите между проектите и приоритетите за изпълнение на проектите на базата на направените констатации.

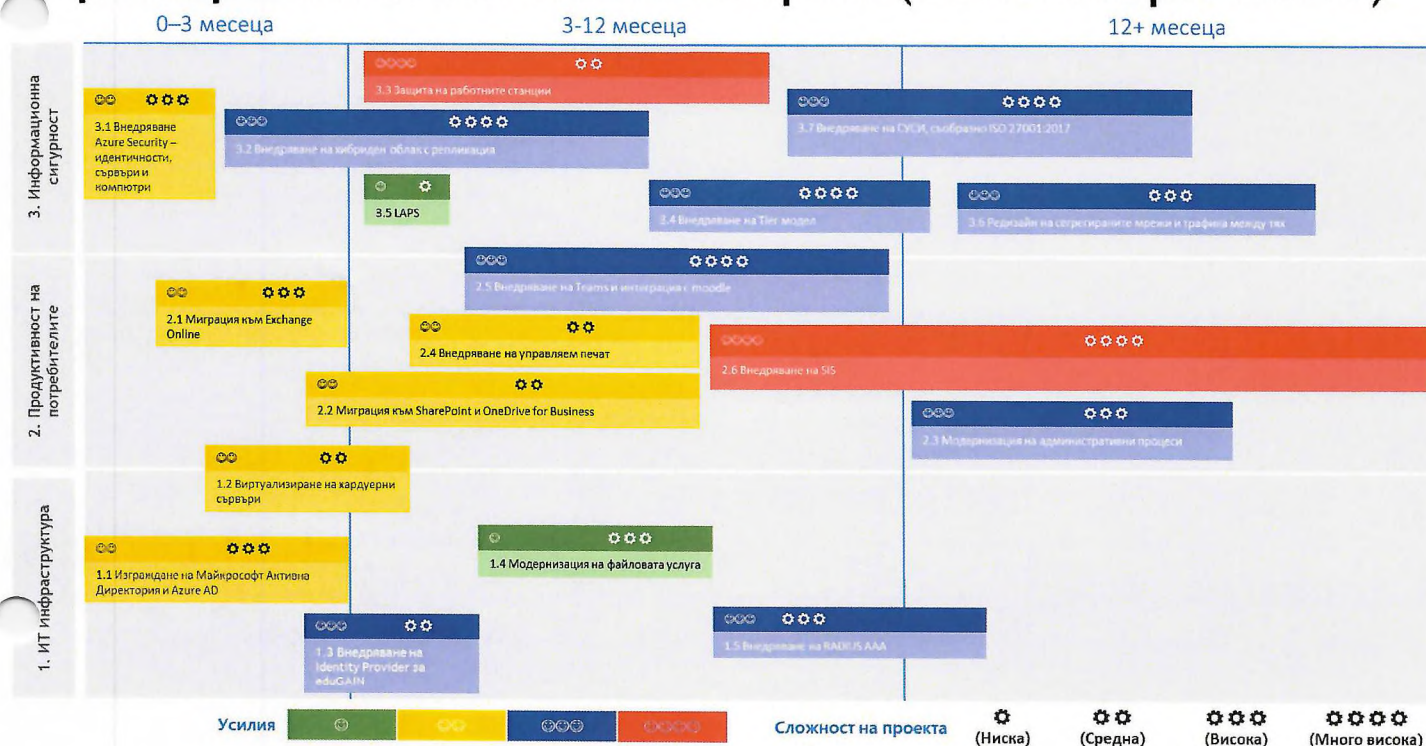
Пътната карта е приложена в Приложение 1.

6. Заключение

Медицински университет – Плевен разполага с добре проектирана и изградена сървърна и мрежова инфраструктура, която отговаря на нужния ресурсен капацитет за изпълнение на дейностите на организацията. Наблюдава се неефективно използване на наличните лицензи. В същото време се използват децентрализирани похвати по отношение на администрирането на системите и колаборацията между служителите, което не отговаря на съвременните норми за бързодействие, ефективно използване на ресурси и ниво на защита на информацията. Наблюдават се редица пропуски в информационната сигурност и управлението на ИТ инфраструктурата. Необходимо е да се наблегне върху създаването на процеси и правила за управление на ИТ както и стандартизация и сигурна среда за работа.

Приложение 1

Препоръчителна пътна карта (септември 2021)



Анализ МУ Плевен - Приложение 2

Package/Severity	Title	Computer	Classification	OS/Platform	Reboot Behavior
Important	RHSA-2021:1469 bind-export-libs_32:9.11.4-26.P2.el7_9.5 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:1469 bind-libs-lite_32:9.11.4-26.P2.el7_9.5 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:1469 bind-license_32:9.11.4-26.P2.el7_9.5 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:3908 cpio_0:2.11-28.el7 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:5002 curl_0:7.29.0-59.el7_9.1 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:4032 dbus_1:1.10.24-15.el7 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:4032 dbus-libs_1:1.10.24-15.el7 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:4011 e2fsprogs_0:1.42.9-19.el7 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:4011 e2fsprogs-libs_0:1.42.9-19.el7 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:3952 expat_0:2.1.0-12.el7 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:3952 expat-devel_0:2.1.0-12.el7 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2020:4907 freetype_0:2.8-14.el7_9.1 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2020:4907 freetype-devel_0:2.8-14.el7_9.1 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:5443 gd_0:2.0.35-27.el7_9 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:5443 gd-devel_0:2.0.35-27.el7_9 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2020:2337 git_0:1.8.3.1-23.el7_8 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:2147 glib2_0:2.56.1-9.el7_9 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:0339 iwl100-firmware_0:39.31.5.1-80.el7_9 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:0339 iwl1000-firmware_1:39.31.5.1-80.el7_9 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:0339 iwl105-firmware_0:18.168.6.1-80.el7_9 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:0339 iwl135-firmware_0:18.168.6.1-80.el7_9 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:0339 iwl2000-firmware_0:18.168.6.1-80.el7_9 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:0339 iwl2030-firmware_0:18.168.6.1-80.el7_9 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:0339 iwl3160-firmware_0:25.30.13.0-80.el7_9 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:0339 iwl3945-firmware_0:15.32.2.9-80.el7_9 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:0339 iwl4965-firmware_0:228.61.2.24-80.el7_9 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:0339 iwl5000-firmware_0:8.83.5.1-1-80.el7_9 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:0339 iwl5150-firmware_0:8.24.2.2-80.el7_9 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:0339 iwl6000-firmware_0:9.221.4.1-80.el7_9 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:0339 iwl6000g2a-firmware_0:18.168.6.1-80.el7_9 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:0339 iwl6000g2b-firmware_0:18.168.6.1-80.el7_9 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:0339 iwl6050-firmware_0:41.28.5.1-80.el7_9 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:0339 iwl7260-firmware_0:25.30.13.0-80.el7_9 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:2725 kernel_0:3.10.0-1160.36.2.el7 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:2725 kernel-tools_0:3.10.0-1160.36.2.el7 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:2725 kernel-tools-libs_0:3.10.0-1160.36.2.el7 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:4011 libcom_err_0:1.42.9-19.el7 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:4011 libcom_err-devel_0:1.42.9-19.el7 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:4072 libcroco_0:0.6.12-6.el7_9 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:5002 libcurl_0:7.29.0-59.el7_9.1 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Low	RHSA-2020:3848 libmspack_0:0.5-0.8.alpha.el7 security update Low	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Low	RHSA-2020:3901 libpng_2:1.5.13-8.el7 security update Low	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Low	RHSA-2020:3901 libpng-devel_2:1.5.13-8.el7 security update Low	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:4011 libss_0:1.42.9-19.el7 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:3915 libssh2_0:1.8.0-4.el7 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:3902 libtiff_0:4.0.3-35.el7 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2020:4908 libX11_0:1.6.7-3.el7_9 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2020:4908 libX11-common_0:1.6.7-3.el7_9 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2020:4908 libX11-devel_0:1.6.7-3.el7_9 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:3996 libxml2_0:2.9.1-6.el7.5 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:3996 libxml2-devel_0:2.9.1-6.el7.5 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:3996 libxml2-python_0:2.9.1-6.el7.5 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:4005 libxslt_0:1.1.28-6.el7 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:0339 linux-firmware_0:20200421-80.git78c0348.el7_9 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:3028 microcode_ctl_2:2.1-73.11.el7_9 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:3972 mod_dev_svn_0:1.7.14-16.el7 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:1145 nettle_0:2.7.1-9.el7_9 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:4076 nsspr_0:4.25.0-2.el7_9 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2021:1384 nss_0:3.53.1-7.el7_9 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:4076 nss-softoken_0:3.53.1-6.el7_9 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:4076 nss-softoken-freebl_0:3.53.1-6.el7_9 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2021:1384 nss-sysinit_0:3.53.1-7.el7_9 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2021:1384 nss-tools_0:3.53.1-7.el7_9 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:4076 nss-util_0:3.53.1-1.el7_9 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2021:1389 openldap_0:2.4.44-23.el7_9 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2020:5566 openssl_1:1.0.2k-21.el7_9 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2020:5566 openssl-devel_1:1.0.2k-21.el7_9 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2020:5566 openssl-libs_1:1.0.2k-21.el7_9 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2021:0343 perl_4:5.16.3-299.el7_9 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2020:2337 perl-Git_0:1.8.3.1-23.el7_8 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2021:0343 perl-libs_4:5.16.3-299.el7_9 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2021:0343 perl-macros_4:5.16.3-299.el7_9 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2021:0343 perl-Pod-Escapes_1:1.04-299.el7_9 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:5009 python_0:2.7.5-90.el7 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:5009 python-libs_0:2.7.5-90.el7 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:2725 python-perf_0:3.10.0-1160.36.2.el7 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:3972 subversion_0:1.7.14-16.el7 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:3972 subversion-libs_0:1.7.14-16.el7 security update Moderate	emis	Security Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:0221 sudo_0:1.8.23-10.el7_9.1 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:0808 wpasupplicant_1:2.6-12.el7_9.2 security update Important	emis	Critical Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:1113 bash_0:4.2.46-34.el7 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:1469 bind-export-libs_32:9.11.4-26.P2.el7_9.5 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:1469 bind-libs_32:9.11.4-26.P2.el7_9.5 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:1469 bind-libs-lite_32:9.11.4-26.P2.el7_9.5 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:1469 bind-license_32:9.11.4-26.P2.el7_9.5 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021:1469 bind-utils_32:9.11.4-26.P2.el7_9.5 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:3908 cpio_0:2.11-28.el7 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:5002 curl_0:7.29.0-59.el7_9.1 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:4032 dbus_1:1.10.24-15.el7 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:4032 dbus-libs_1:1.10.24-15.el7 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:4011 e2fsprogs_0:1.42.9-19.el7 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:4011 e2fsprogs-libs_0:1.42.9-19.el7 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020:3952 expat_0:2.1.0-12.el7 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2020:4907 freetype_0:2.8-14.el7_9.1 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)	
Low	RHSA-2020:1138 gettext_0:0.19.8.1-3.el7 security update Low	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)	

Low	RHSA-2020:1138 gettext-libs_0:0.19.8.1-3.el7 security update Low	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:2147 glib2_0:2.56.1-9.el7_9 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl100-firmware_0:39.31.5.1-80.el7_9 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl1000-firmware_1:39.31.5.1-80.el7_9 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl105-firmware_0:18.168.6.1-80.el7_9 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl135-firmware_0:18.168.6.1-80.el7_9 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl2000-firmware_0:18.168.6.1-80.el7_9 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl2030-firmware_0:18.168.6.1-80.el7_9 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl3160-firmware_0:25.30.13.0-80.el7_9 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl3945-firmware_0:15.32.2.9-80.el7_9 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl4965-firmware_0:228.61.2.24-80.el7_9 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl5000-firmware_0:8.83.5.1_1-80.el7_9 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl5150-firmware_0:8.24.2.2-80.el7_9 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl6000-firmware_0:9.221.4.1-80.el7_9 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl6000g2a-firmware_0:18.168.6.1-80.el7_9 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl6000g2b-firmware_0:18.168.6.1-80.el7_9 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl6050-firmware_0:41.28.5.1-80.el7_9 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl7260-firmware_0:25.30.13.0-80.el7_9 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:2725 kernel_0:3.10.0-1160.36.2.el7 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:2725 kernel-tools_0:3.10.0-1160.36.2.el7 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:2725 kernel-tools-libs_0:3.10.0-1160.36.2.el7 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4011 libcom_err_0:1.42.9-19.el7 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4072 libcroco_0:0.6.12-6.el7_9 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:5002 libcurl_0:7.29.0-59.el7_9.1 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2020:0897 libicu_0:50.2.4-4.el7_7 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2019:2052 libjpeg-turbo_0:2.90.8-1.el7 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Low	RHSA-2020:3848 libmspack_0:0.5-0.8.alpha.el7 security update Low	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Low	RHSA-2020:3901 libpng_2:1.5.13-8.el7 security update Low	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4011 libss_0:1.42.9-19.el7 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:3915 libssh2_0:1.8.0-4.el7 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:3902 libtiff_0:4.0.3-35.el7 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2020:4908 libx11_0:1.6.7-3.el7_9 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2020:4908 libx11-common_0:1.6.7-3.el7_9 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:3996 libxml2_0:2.9.1-6.el7.5 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:3996 libxml2-python_0:2.9.1-6.el7.5 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4005 libxslt_0:1.1.28-6.el7 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 linux-firmware_0:20200421-80.git78c0348.el7_9 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:3028 microcode_ctl_2:2.1-73.11.el7_9 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2020:5350 net-snmp_1:5.7.2-49.el7_9.1 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2020:5350 net-snmp-agent-libs_1:5.7.2-49.el7_9.1 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2020:5350 net-snmp-libs_1:5.7.2-49.el7_9.1 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2020:5350 net-snmp-utils_1:5.7.2-49.el7_9.1 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4076 nspr_0:4.25.0-2.el7_9 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2021:1384 nss_0:3.53.1-7.el7_9 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4076 nss-softokn_0:3.53.1-6.el7_9 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4076 nss-softokn-freebl_0:3.53.1-6.el7_9 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2021:1384 nss-sysinit_0:3.53.1-7.el7_9 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2021:1384 nss-tools_0:3.53.1-7.el7_9 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4076 nss-utils_0:3.53.1-1.el7_9 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2021:1389 openssl_0:2.4.44-23.el7_9 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Low	RHSA-2019:2143 openssl_0:7.4p1-21.el7 security update Low	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Low	RHSA-2019:2143 openssl-clients_0:7.4p1-21.el7 security update Low	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Low	RHSA-2019:2143 openssl-server_0:7.4p1-21.el7 security update Low	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2020:5566 openssl_1:1.0.2k-21.el7_9 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2020:5566 openssl-libs_1:1.0.2k-21.el7_9 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2021:0343 perl_4:5.16.3-299.el7_9 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2021:0343 perl-libs_4:5.16.3-299.el7_9 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2021:0343 perl-macros_4:5.16.3-299.el7_9 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2021:0343 perl-Pod-Escapes_1:1.04-299.el7_9 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Low	RHSA-2020:1135 polkit_0:0.112-26.el7 security update Low	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:5009 python_0:2.7.5-90.el7 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:5009 python-libs_0:2.7.5-90.el7 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:2725 python-perf_0:3.10.0-1160.36.2.el7 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:1021 shared-mime-info_0:1.8-5.el7 security update Moderate	mdsc	Security Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2020:0227 sqlite_0:3.7.17-8.el7_7.1 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0221 sudo_0:1.8.23-10.el7_9.1 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0808 wpasupplicant_1:2.6-12.el7_9.2 security update Important	mdsc	Critical Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:1113 bash_0:4.2.46-34.el7 security update Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:3908 cpio_0:2.11-28.el7 security update Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:5002 curl_0:7.29.0-59.el7_9.1 security update Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4011 e2fsprogs_0:1.42.9-19.el7 security update Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4011 e2fsprogs-libs_0:1.42.9-19.el7 security update Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:3952 expat_0:2.1.0-12.el7 security update Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:3952 expat-devel_0:2.1.0-12.el7 security update Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2020:4907 freetype_0:2.8-14.el7_9.1 security update Important	mail	Critical Updates	CentOS Linux 7.0 (x86_64)
Low	RHSA-2020:1138 gettext_0:0.19.8.1-3.el7 security update Low	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Low	RHSA-2020:1138 gettext-libs_0:0.19.8.1-3.el7 security update Low	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:2147 glib2_0:2.56.1-9.el7_9 security update Important	mail	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl100-firmware_0:39.31.5.1-80.el7_9 security update Important	mail	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl105-firmware_0:18.168.6.1-80.el7_9 security update Important	mail	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl135-firmware_0:18.168.6.1-80.el7_9 security update Important	mail	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl2000-firmware_0:18.168.6.1-80.el7_9 security update Important	mail	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl2030-firmware_0:18.168.6.1-80.el7_9 security update Important	mail	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl3160-firmware_0:25.30.13.0-80.el7_9 security update Important	mail	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl3945-firmware_0:15.32.2.9-80.el7_9 security update Important	mail	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl4965-firmware_0:228.61.2.24-80.el7_9 security update Important	mail	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl5000-firmware_0:8.83.5.1_1-80.el7_9 security update Important	mail	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl5150-firmware_0:8.24.2.2-80.el7_9 security update Important	mail	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl6000-firmware_0:9.221.4.1-80.el7_9 security update Important	mail	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl6000g2a-firmware_0:18.168.6.1-80.el7_9 security update Important	mail	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl6000g2b-firmware_0:18.168.6.1-80.el7_9 security update Important	mail	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl6050-firmware_0:41.28.5.1-80.el7_9 security update Important	mail	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iwl7260-firmware_0:25.30.13.0-80.el7_9 security update Important	mail	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:2725 kernel_0:3.10.0-1160.36.2.el7 security update Important	mail	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:2725 kernel-tools_0:3.10.0-1160.36.2.el7 security update Important	mail	Critical Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4011 libcom_err_0:1.42.9-19.el7 security update Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4011 libcom_err-devel_0:1.42.9-19.el7 security update Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4072 libcroco_0:0.6.12-6.el7_9 security update Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)

Moderate	RHSA-2020:5002 libcurl_0.7.29.0-59.el7_9.1 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2020:0897 libicu_0.50.2-4.el7_7 security update	Important	mail	Critical Updates	CentOS Linux 7.0 (x86_64)
Low	RHSA-2020:3848 libmspack_0.0.5-0.8.alpha.el7 security update	Low	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4011 libss_0.1.42.9-19.el7 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:3915 libssh2_0.1.8.0-4.el7 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2020:4908 libX11_0.1.6.7-3.el7_9 security update	Important	mail	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2020:4908 libX11-common_0.1.6.7-3.el7_9 security update	Important	mail	Critical Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:3996 libxml2_0.2.9.1-6.el7.5 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4005 libxslt_0.1.1.28-6.el7 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 linux-firmware_0.20200421-80.git78c0348.el7_9 security update	Important	mail	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:1145 nettle_0.2.7.1-9.el7_9 security update	Important	mail	Critical Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4076 nspr_0.4.25.0-2.el7_9 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2021:1384 nss_0.3.53.1-7.el7_9 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4076 nss-softokn_0.3.53.1-6.el7_9 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4076 nss-softokn-freebl_0.3.53.1-6.el7_9 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2021:1384 nss-sysinit_0.3.53.1-7.el7_9 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2021:1384 nss-tools_0.3.53.1-7.el7_9 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4076 nss-util_0.3.53.1-1.el7_9 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2021:1389 openssl_0.2.4.44-23.el7_9 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2021:0343 perl-ExtUtils-Install_0.1.58-259.el7_9 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:1112 php_0.5.4.16-48.el7 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:1112 php-bcmath_0.5.4.16-48.el7 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:1112 php-cli_0.5.4.16-48.el7 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:1112 php-common_0.5.4.16-48.el7 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:1112 php-gd_0.5.4.16-48.el7 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:1112 php-intl_0.5.4.16-48.el7 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:1112 php-ldap_0.5.4.16-48.el7 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:1112 php-mbstring_0.5.4.16-48.el7 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:1112 php-mysql_0.5.4.16-48.el7 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:1112 php-pdo_0.5.4.16-48.el7 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:1112 php-process_0.5.4.16-48.el7 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:1112 php-pspell_0.5.4.16-48.el7 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:1112 php-xml_0.5.4.16-48.el7 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Low	RHSA-2020:1135 polkit_0.102.112-26.el7 security update	Low	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:5009 python_0.2.7.5-90.el7 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:5009 python-libs_0.2.7.5-90.el7 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:2725 python-perf_0.3.10.0-1160.36.2.el7 security update	Important	mail	Critical Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:1021 shared-mime-info_0.1.8-5.el7 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:3973 spamassassin_0.3.4.0-6.el7 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:3972 subversion_0.1.7.14-16.el7 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:3972 subversion-libs_0.1.7.14-16.el7 security update	Moderate	mail	Security Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0221 sudo_0.1.8.23-10.el7_9.1 security update	Important	mail	Critical Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:1113 bash_0.4.2.46-34.el7 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:1469 bind-libs-lite_32.9.11.4-26.P2.el7_9.5 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:1469 bind-license_32.9.11.4-26.P2.el7_9.5 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:3908 cpio_0.2.11-28.el7 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:5002 curl_0.7.29.0-59.el7_9.1 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4032 dbus_1.11.10-24-15.el7 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4032 dbus-libs_1.11.10-24-15.el7 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:3952 expat_0.2.1.0-12.el7 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2020:4907 freetype_0.2.8-14.el7_9.1 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Low	RHSA-2020:1138 gettext_0.19.8.1-3.el7 security update	Low	www	Security Updates	CentOS Linux 7.0 (x86_64)
Low	RHSA-2020:1138 gettext-libs_0.19.8.1-3.el7 security update	Low	www	Security Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:2147 glib2_0.2.56.1-9.el7_9 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iw1000-firmware_0.39.31.5.1-80.el7_9 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iw1000-firmware_1.39.31.5.1-80.el7_9 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iw105-firmware_0.18.168.6.1-80.el7_9 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iw1135-firmware_0.18.168.6.1-80.el7_9 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iw12000-firmware_0.18.168.6.1-80.el7_9 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iw12030-firmware_0.18.168.6.1-80.el7_9 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iw13160-firmware_0.25.30.13.0-80.el7_9 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iw13945-firmware_0.15.32.2.9-80.el7_9 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iw14565-firmware_0.228.61.2.24-80.el7_9 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iw15150-firmware_0.8.24.2.2-80.el7_9 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iw16000-firmware_0.9.221.4.1-80.el7_9 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iw16000g2a-firmware_0.18.168.6.1-80.el7_9 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iw16000g2b-firmware_0.18.168.6.1-80.el7_9 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iw16050-firmware_0.41.28.5.1-80.el7_9 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 iw17260-firmware_0.25.30.13.0-80.el7_9 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:2725 kernel_0.3.10.0-1160.36.2.el7 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:2725 kernel-tools_0.3.10.0-1160.36.2.el7 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:2725 kernel-tools-libs_0.3.10.0-1160.36.2.el7 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4072 libcroco_0.0.6.12-6.el7_9 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:5002 libcurl_0.7.29.0-59.el7_9.1 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2020:0897 libicu_0.50.2-4.el7_7 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2019:2052 libjpeg-turbo_0.1.2.90-8.el7 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)
Low	RHSA-2020:3848 libmspack_0.0.5-0.8.alpha.el7 security update	Low	www	Security Updates	CentOS Linux 7.0 (x86_64)
Low	RHSA-2020:3901 libpng_2.1.5.13-8.el7 security update	Low	www	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:3915 libssh2_0.1.8.0-4.el7 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:3902 libtiff_0.4.0.3-35.el7 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2020:4908 libX11_0.1.6.7-3.el7_9 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2020:4908 libX11-common_0.1.6.7-3.el7_9 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4005 libxslt_0.1.1.28-6.el7 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:0339 linux-firmware_0.20200421-80.git78c0348.el7_9 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Important	RHSA-2021:3028 microcode_ctl_2.12.1-73.11.el7_9 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4076 nspr_0.4.25.0-2.el7_9 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2021:1384 nss_0.3.53.1-7.el7_9 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4076 nss-softokn_0.3.53.1-6.el7_9 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4076 nss-softokn-freebl_0.3.53.1-6.el7_9 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2021:1384 nss-sysinit_0.3.53.1-7.el7_9 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2021:1384 nss-tools_0.3.53.1-7.el7_9 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2020:4076 nss-util_0.3.53.1-1.el7_9 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2021:1389 openssl_0.2.4.44-23.el7_9 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)
Low	RHSA-2019:2143 openssl_0.7.4p1-21.el7 security update	Low	www	Security Updates	CentOS Linux 7.0 (x86_64)
Low	RHSA-2019:2143 openssl-clients_0.7.4p1-21.el7 security update	Low	www	Security Updates	CentOS Linux 7.0 (x86_64)
Low	RHSA-2019:2143 openssl-server_0.7.4p1-21.el7 security update	Low	www	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2021:0343 perl_4.15.16.3-299.el7_9 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)
Moderate	RHSA-2021:0343 perl-libs_4.15.16.3-299.el7_9 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)

Moderate	RHSA-2021-0343 perl-macros_4.15.16.3-299.el7_9 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2021-0343 perl-Pod-Escapes_1.1.04-299.el7_9 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)	
Low	RHSA-2020-1135 polkit_0.10.112-26.el7 security update	Low	www	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020-5009 python_0.2.7.5-90.el7 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020-5009 python-libs_0.2.7.5-90.el7 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021-2725 python-perf_0.3.10.0-1160.36.2.el7 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020-1021 shared-mime-info_0.1.8-5.el7 security update	Moderate	www	Security Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2020-0227 sqlite_0.3.7.17-8.el7_7.1 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021-0221 sudo_0.1.8.23-10.el7_9.1 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021-0808 wpa_supplicant_1:2.6-12.el7_9.2 security update	Important	www	Critical Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020-1113 bash_0.4.2.46-34.el7 security update	Moderate	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020-3908 cpio_0.2.11-28.el7 security update	Moderate	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020-5002 curl_0.7.29.0-59.el7_9.1 security update	Moderate	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020-4011 e2fsprogs_0.1.42.9-19.el7 security update	Moderate	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020-4011 e2fsprogs-libs_0.1.42.9-19.el7 security update	Moderate	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020-3952 expat_0.2.1.0-12.el7 security update	Moderate	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2020-4907 freetype_0.2.8-14.el7_9.1 security update	Important	ns	Critical Updates	CentOS Linux 7.0 (x86_64)	
Low	RHSA-2020-1138 gettext_0.0.19.8.1-3.el7 security update	Low	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Low	RHSA-2020-1138 gettext-libs_0.0.19.8.1-3.el7 security update	Low	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021-2147 glib2_0.2.56.1-9.el7_9 security update	Important	ns	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021-0339 iwl100-firmware_0:39.31.5.1-80.el7_9 security update	Important	ns	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021-0339 iwl105-firmware_0:18.168.6.1-80.el7_9 security update	Important	ns	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021-0339 iwl135-firmware_0:18.168.6.1-80.el7_9 security update	Important	ns	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021-0339 iwl2000-firmware_0:18.168.6.1-80.el7_9 security update	Important	ns	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021-0339 iwl2030-firmware_0:18.168.6.1-80.el7_9 security update	Important	ns	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021-0339 iwl3160-firmware_0:25.30.13.0-80.el7_9 security update	Important	ns	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021-0339 iwl3945-firmware_0:15.32.2.9-80.el7_9 security update	Important	ns	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021-0339 iwl4965-firmware_0:228.61.2.24-80.el7_9 security update	Important	ns	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021-0339 iwl5000-firmware_0:8.83.5.1-1-80.el7_9 security update	Important	ns	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021-0339 iwl5150-firmware_0:8.24.2.2-80.el7_9 security update	Important	ns	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021-0339 iwl6000-firmware_0:9.221.4.1-80.el7_9 security update	Important	ns	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021-0339 iwl6000g2a-firmware_0:18.168.6.1-80.el7_9 security update	Important	ns	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021-0339 iwl6000g2b-firmware_0:18.168.6.1-80.el7_9 security update	Important	ns	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021-0339 iwl6050-firmware_0:41.28.5.1-80.el7_9 security update	Important	ns	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021-0339 iwl7260-firmware_0:25.30.13.0-80.el7_9 security update	Important	ns	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021-2725 kernel_0.3.10.0-1160.36.2.el7 security update	Important	ns	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021-2725 kernel-tools_0.3.10.0-1160.36.2.el7 security update	Important	ns	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021-2725 kernel-tools-libs_0.3.10.0-1160.36.2.el7 security update	Important	ns	Critical Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2019-2047 libgroup_0.0.41-21.el7 security update	Moderate	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020-4011 libcom_err_0.1.42.9-19.el7 security update	Moderate	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020-4072 libcroc_0.0.6.12-6.el7_9 security update	Moderate	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020-5002 libcurl_0.7.29.0-59.el7_9.1 security update	Moderate	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2020-0897 libicu_0.50.2-4.el7_7 security update	Important	ns	Critical Updates	CentOS Linux 7.0 (x86_64)	
Low	RHSA-2020-3848 libmspack_0.0.5-0.8.alpha.el7 security update	Low	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020-4011 libss_0.1.42.9-19.el7 security update	Moderate	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020-3915 libssh2_0.1.8.0-4.el7 security update	Moderate	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020-3996 libxml2_0.2.9.1-6.el7.5 security update	Moderate	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020-4005 libxslt_0.1.1.28-6.el7 security update	Moderate	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021-0339 linux-firmware_0:20200421-80.git78c0948.el7_9 security update	Important	ns	Critical Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020-4076 nssr_0.4.25.0-2.el7_9 security update	Moderate	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2021-1384 nss_0.3.53.1-7.el7_9 security update	Moderate	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020-4076 nss-softoken_0.3.53.1-6.el7_9 security update	Moderate	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020-4076 nss-softoken-freebl_0.3.53.1-6.el7_9 security update	Moderate	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2021-1384 nss-sysinit_0.3.53.1-7.el7_9 security update	Moderate	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2021-1384 nss-tools_0.3.53.1-7.el7_9 security update	Moderate	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020-4076 nss-util_0.3.53.1-1.el7_9 security update	Moderate	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2021-1389 openldap_0.2.4.44-23.el7_9 security update	Moderate	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Low	RHSA-2019-2143 openssh-clients_0.7.4p1-21.el7 security update	Low	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Low	RHSA-2019-2143 openssh-server_0.7.4p1-21.el7 security update	Low	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Low	RHSA-2020-1135 polkit_0.0.112-26.el7 security update	Low	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020-5009 python_0.2.7.5-90.el7 security update	Moderate	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020-5009 python-libs_0.2.7.5-90.el7 security update	Moderate	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021-2725 python-perf_0.3.10.0-1160.36.2.el7 security update	Important	ns	Critical Updates	CentOS Linux 7.0 (x86_64)	
Moderate	RHSA-2020-1021 shared-mime-info_0.1.8-5.el7 security update	Moderate	ns	Security Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2020-0227 sqlite_0.3.7.17-8.el7_7.1 security update	Important	ns	Critical Updates	CentOS Linux 7.0 (x86_64)	
Important	RHSA-2021-0221 sudo_0.1.8.23-10.el7_9.1 security update	Important	ns	Critical Updates	CentOS Linux 7.0 (x86_64)	
	2021-08 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5005043)		WIN-M1T01GTSVFT	Security Updates	Windows Server 2016	CanRequestReboot
	2021-04 Servicing Stack Update for Windows Server 2016 for x64-based Systems (KB5001402)		WIN-9AJGMHR617I	Security Updates	Windows Server 2016	NeverReboots
	Security Update for Windows Server 2016 for x64-based Systems (KB4535680)		WIN-9AJGMHR617I	Security Updates	Windows Server 2016	CanRequestReboot
	2020-01 Security and Quality Rollup for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows 7		WSS-MUPleven	Security Updates	Windows Server 2008 R2	CanRequestReboot
	2019-03 Servicing Stack Update for Windows Server 2008 R2 for x64-based Systems (KB4490628)		WSS-MUPleven	Security Updates	Windows Server 2008 R2	NeverReboots
	2020-01 Servicing Stack Update for Windows Server 2008 R2 for x64-based Systems (KB4536952)		WSS-MUPleven	Security Updates	Windows Server 2008 R2	NeverReboots
	2019-10 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems (KB4524157)		WSS-MUPleven	Security Updates	Windows Server 2008 R2	CanRequestReboot
	2018-02 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems (KB4074598)		WSS-MUPleven	Security Updates	Windows Server 2008 R2	CanRequestReboot

План за „Извършване на анализ на съответствието (GAP анализ) на наличната ИТ инфраструктура“

I. Цели и обхват на предоставяната услуга

1.1. Общи и специфични цели на проекта

„Извършване на анализ на съответствието (GAP анализ) на наличната ИТ инфраструктура“ е инструмент за стратегическо планиране, който Ви предоставя възможност да разберете къде се намира организацията Ви в на този етап, къде искате да бъде и как ще стигнете до там. Анализът има за цел да представи на ръководството текущото състояние на информационната архитектура, използвани технологии, ресурсната обезпеченост на информационните процеси, налични приложения и свързаните с тях ресурси за осигуряване на информацията, както и процеси за осигуряване на сигурността. На базата на анализа ще бъдат формулирани предложения за надграждане и подобряване, съгласно добрите практики, стандарти и законови рамки. Резултатите от анализа ще предоставят възможност на ръководството на [Company] за вземане на информирани решения, дефиниране на ИТ стратегия за развитие и пътна карта за нейното изпълнение с ясни приоритети и времева рамка, спрямо текущото състояние на инфраструктурата.

1.2. Обхват на проекта

Анализът ще обхване цялата налична ИТ инфраструктура - сървърна, дискова, комуникационна, системен и приложен софтуер както и свързаните с тях ИТ процеси в институцията. В обхвата не е включен преглед на служебните работни станции и мобилни устройства, освен ако не са част от система за управление на устройства (MDM). Следните точки ще бъдат включени:

1.2.1. Текущо състояние

Снемане на текущата обстановка и анализ на данните, на базата на което ще бъдат изготвени констатации за състоянието на всяка една от следните позиции:

- **Хардуерен слой** - проучване и анализ на наличния хардуер, използването му, амортизация, цикъл на поддръжка;
- **Инфраструктурен софтуерен слой** – проучване на наличните инфраструктурни системи, системи за управление на идентичностите, системи за защита, софтуер за наблюдение и известяване и други софтуери, осигуряващи среда за работа на приложния слой;
- **Инфраструктурен мрежови слой** – включва проучване и анализ на наличната мрежова инфраструктура, устойчивост, ниво на сигурност, използваемост и капацитет;

- **Приложен софтуер** – проучва се текущия приложен софтуер и прилежащите му данни;
- **Непрекъсваемост на системите** – анализират се текущите заложи мерки и правила за осигуряване на непрекъсваемост на системите.

1.2.2. Констатации по текущото състояние

Изготвяне на списък от констатации по текущото състояние на информационните системи.

1.2.3. Препоръки за подобрене

- **Визия** – определя се желаното бъдещо състояние, спрямо целите на организацията и добрите практики, стандарти, законовите рамки;
- **Инициативи** – изготвят се списък от препоръки и инициативи за постигане на желания дизайн на инфраструктурата, спрямо заложената визия;
- **Пътна карта** – изготвя се пътна карта и свързаните с визията и инициативите проекти. Освен описанието, за всеки проект се определя приоритет, сложност, необходим софтуер и хардуер.

II. План на одита

2.1. Одитори

Име	Младен Георгиев	Роля	Водещ одитор
Е-мейл	Mladen.Georgiev@MYSynergy.bg	Телефон	+359 889 5000 80
Име	Ростислав Русинов	Роля	Одитор
Е-мейл	Rostislav.Rusinov@MYSynergy.bg	Телефон	+359 88 555 4022
Име	Николай Шарков	Роля	Одитор
Е-мейл	Nikolay.Sharkov@MYSynergy.bg	Телефон	+359 876 378 023

2.2. Период и място на провеждане

Одитът ще бъде проведен на място в МУ Плевен в рамките на **2 дни** в периода **10 – 11 август 2021** година през работното време на ИТ отдела от 8:00 до 16:30 часа. Може да бъде проведена и допълнителна уточняваща среща онлайн, която ще бъде уточнена предварително.

2.3. Одитирани области

Област	Одитор	Ден
Съответствие спрямо нормативни и договорени изисквания	Младен Георгиев	10.08
Опис на оборудване в център за данни: - Сървъри - Дискови масиви - UPS - Пожароизвестяване, гасене, наблюдение на температура и др.	Ростислав Русинов	10.08
Инсталация на агенти за анализ работата на сървъри и системи	Ростислав Русинов Николай Шарков	11.08
Опис на мрежово оборудване: - В център за данни - Сградна инфраструктура	Николай Шарков	10.08
Инфраструктурен софтуерен слой	Младен Георгиев	11.08
Приложен софтуер	Младен Георгиев	11.08