

Република Србија
Академија техничко-васпитачких
струковних студија – одсек Ниш
Број: 02-1/263
Датум: 26.08.2020. године

На основу Закона о заштити података о личности („Службени гласник РС“ бр. 87/2018) и члана 3 и члана 4. Закона о слободном приступу информацијама од јавног значаја („Службени гласник РС“ број 120/2004, 54/2007, 104/2009 и 36/2010), и члана 65. Статута Академије техничко-васпитачких струковних студија (Печишћен текст број:01-1/9-1 од 21.01.2020. године, в.д. председника Академије техничко-васпитачких струковних студија доноси следећи

П РА В И Л Н И К

о примени видео надзора којим се контролише приступ у службени простор Академије техничко-васпитачких струковних студија – одсек Ниш

Члан 1.

Овим Правилником регулисана је примена видео надзора којим се контролише приступ у службени односно пословни простор Академије техничко-васпитачких струковних студија – одсек Ниш (У даљем тексту: Академија – одсек Ниш), ради безбедности лица и имовине, контроле уласка или изласка из службеног односно пословног простора Академије-одсек Ниш.

Члан 2.

Одлуку о увођењу видео надзора доноси руководилац Осека уз претходну сагласност органа председника Академије техничко-васпитачких струковних студија.

Члан 3.

Академија – одсек Ниш је у обавези да истакне јавно обавештење да се врши видео надзор. Обавештење мора бити истакнуто на видном месту, на начин који омогућава лицима да се са вршењем видео надзора упознају.

Обавештење да се врши видео надзор садржи податке о:

- 1) лицу које врши видео надзор;
- 2) броју телефона на који се могу добити информације где се и колико дуго чувају снимци из система видео надзора.

Истицањем обавештења сматра се да је лице обавештено о обради личних података.

Члан 4.

Запослени који раде у просторијама под видео надзором, морају бити у писаном облику обавештени о вршењу видео надзора.

Члан 5.

Систем видео надзора мора бити заштићен од приступа неовлашћених лица.

Лице које врши видео надзор у обавези је да:

1. буде прописно обучен за вршење неопходних радњи на систему;
2. прочита, разуме и придржава се свих сигурносних процедура о сигурном раду информацијско-комуникацијских система;
3. пријави сваки сигурносни инцидент или необичан догађај који се може опазити током рада информацијско-комуникацијског система.

Члан 6.

Евиденција видео надзора садржи: снимак лица (слику), датум и време снимања. Подаци из евиденције чувају се, по правилу, најдуже месец дана од дана настанка.

Члан 7.

Снимци података прикупљених уз помоћ видео надзора обрађују се и користе у складу са Законом којим се уређује заштита података о личности.

Члан 8.

У случају да постоји сумња да снимљени подаци могу представљати доказ у кривичном или прекршајном поступку, дисциплинском поступку, за утврђивање стварног стања у жалбеним поступцима или код утврђивања могуће материјалне одговорности, снимци података прикупљени уз помоћ видео надзора се копирају на CD или електронски обрађују на други начин.

Члан 9.

Захтев за копирање података прикупљених уз помоћ видео надзора их претходног члана могу поднети:

1. органи гоњења Републике Србије,
2. надзорни органи за заштиту података о личности Републике Србије и
3. свако заинтересовано лице које учини вероватним да снимак може представљати доказ у кривичном или прекршајном, дисциплинском поступку, за утврђивање стварног стања у жалбеним поступцима или код утврђивања могуће материјалне одговорности.

У случају да захтев из претходног става подноси лице из тачке 3., захтев се подноси руководиоцу одсека у писаној форми, који процењује да ли су разлози наведени у захтеву оправдани или не. Уколико руководиоца одсека процени да је захтев оправдан донеће одлуку копирању или електронској обради података прикупљених уз помоћ видео надзора.

Члан 10.

Подаци који су копирани или на други начин електронски обрађени комисијски се уништавају након престанка разлога због којих је извршено копирање или електронска обрада података.

Члан 11.

Злоупотреба података прикупљених уз помоћ видео надзора, односно употреба ових података супротно одредбама Закона о заштити података о личности, Закона о слободном приступу информацијама од јавног значаја и одредаба овог Правилника, подлеже кривичној и дисциплинској одговорности лица које је злоупотребило ове податке.

Члан 12.

Забрањен је приступ снимцима система видео надзора преко интерне кабловске телевизије, јавне кабловске телевизије, интернета, или других средстава за телекомуникацију којима се такви снимци могу пренети, било у тренутку њиховог настанка или након тога

Приступ снимцима система видео надзора преко интерне кабловске телевизије, јавне кабловске телевизије, интернета, или других средстава за телекомуникацију подлеже кривичној и дисциплинској одговорности.

Члан 13.

Саставни део овог Правилника је Извештај о употреби и локацијама система видео надзора у објекту Академије – одсек.

Овај Правилник ступа на снагу даном објављивања на WEB страници Академије-одсек Ниш.



В.Д. председника Академије техничко-
васпитачких струковних студија
Александар Саша
проф. др Саша Николић

ИЗВЕШТАЈ О УПОТРЕБИ И ЛОКАЦИЈАМА СИСТЕМА ВИДЕО НАДЗОРА У ОБЈЕКТУ АКАДЕМИЈЕ ТЕХНИЧКО-ВАСПИТАЧКИХ СТРУКОВНИХ СТУДИЈА-ОДСЕК НИШ

УПОТРЕБА СИСТЕМА ВИДЕО НАДЗОРА НА ПРОСТОРУ АКАДЕМИЈЕ ТЕХНИЧКО-ВАСПИТАЧКИХ СТРУКОВНИХ СТУДИЈА-ОДСЕК НИШ

Видео надзор је стандардни елемент физичко-техничког обезбеђења имовине сваке установе, заштите радног окружења запослених и заштите безбедности студената и запослених. Намена снимака видео надзора јесте само за визуелне контроле периметра и просторија објекта. Снимци лица снимљених видео камерама не обрађују се ни у какве друге сврхе, осим за контролу физичке безбедности периметра и просторија објекта.

Систем видео надзора на простору Академије биће коришћен за:

- Одржавање безбедног окружења Академије.
- Осигурање безбедности ученика и запослених.
- Одвраћање од криминалног понашања и насиља према људима и имовини Академије.
- Помоћ полицији у идентификовању лица која чине насиље и друге прекршаје.

Систем видео надзора на простору Академије биће регистрован према законима и прописима Републике Србије. Ознаке упозорења на коришћење система за видео надзор биће постављене у свим просторијама и окружењу Академије.

Безбедност система видео надзора:

- Видео надзор се неће користити за контролу појединаца све док се не захтева непосредан одговор на инцидент.
- Систем видео надзора неће се користити за приватна возила, појединце или имовину изван периметра Академије
- Видео снимци ће се репродуковати само на писани захтев овлашћених лица из полиције или на захтев овлашћених лица за контролу приступа Академији.
- Приступ систему видео надзора, софтверу и подацима је рестриктиван, биће заштићен јаком лозинком и ограничен само за овлашћена лица.
- Главна контролна платформа Система видео надзора чуваће се на безбедном месту и закључавати када није у употреби.
- Видео монитори система биће лоцирани у канцеларији ИТ службе (104) и канцеларији домара објекта (210).

Пракса употребе система видео надзора

Академија ће инсталирати систем видео надзора у циљу спречавања и откривања криминалних активности и у циљу сигурности и добробити запослених, студената и посетиоца. Власник видео надзора је Академија, а видео записи се стриктно контролишу и надгледају од стране овлашћеног лица.

Систем видео надзора ће:

- се увек користити за спецификоване намене и легитимне циљеве,
- бити дизајниран и конфигуриран тако да узима у обзир утицај на појединце, заштиту њихове приватности и података о личности,
- бити транспарентан и укључиваће приступну тачку за приступ информацијама и за притужбе лица,
- имати јасну одговорност и контролу над сликама и скупљеним видео снимцима, задржаваним и коришћеним информацијама и документацијом,

- имати дефинисану политику и процедуре на видљивом месту за све запослене и студенте у Академији,
- задржавати информације само онолико колико се захтева,
- спречити неовлашћен приступ задржаваним сликама и информацијама у складу са јасним правилима о томе ко може добити приступ,
- разматрати све оперативне, техничке и конкурентне стандарде релевантне за систем видео надзора, његову намену и рад да задовољи и одржава ове стандарде у складу са законом,
- бити обавезан да појача мере заштите од неовлашћеног приступа и употребе,
- бити регуларно провераван и испитиван да се осигура спровођење политике и стандарда,
- бити употребљен само за сврхе за које су намењене, укључујући подршку јавној сигурности, заштити студената и запослених, полицији и другим органима истраге,
- бити тачан и добро одржаван да осигура ажурне информације и податке о личности.

Заштита приватности студената и запослених Академије техничко-васпитачких струковних студија - Одсек Ниш

- Активни и снимљени видео материјали могу гледати само овлашћени оператери за потребе истраге инцидента.
- Фотографије и видео снимци могу се достављати полицији за откривање криминалног понашања.
- Свако гледање снимака од стране полиције треба евидентирати у дневник рада система (лог датотеку).
- Сваки захтев или апликацију примљену од других тела (нпр. адвоката) за гледање или достављање снимака видео надзора треба доставити руководиоцу Академије.
- У случају када трећа страна захтева да види или добије снимке, Руководиоц ће испунити захтев уз одговарајућу документацију да су докази достављени по захтеву за закониту истрагу, или захтеву лица за приступ, или као одговор на судски позив.
- Видео снимци ће се задржавати толико дуго колико се захтева. Систем видео надзора ће аутоматски избрисати све снимке после 30. дана у складу са Законом о физичко-техничком обезбеђењу Републике Србије.

ПРОЦЕНА РИЗИКА РАДЊИ ОБРАДЕ ВИДЕО НАДЗОРА

Академија техничко-васпитачких струковних студија-Одсек Ниш обрађује податке о личности слике и видео записе у систему видео надзора за обезбеђење физичког приступа радним просторијама. Претпоставља се да Академија неће врши никакву легалну анализу на бази видео надзора и да је обрада личних подата усаглашена са важећим законима и прописима у овој области.

Систем видео надзора ће се састојати се од камера које снимају секвенце, приказује их оператеру физичке безбедности и логује све активности обраде снимљеног материјала.

Видео снимци ће се складиштити до 30 дана, затим се аутоматски безбедно бришу, осим ако их оператер не извлачи мануелно, нпр. у случају аларма у ванредном стању.

Оператер платформе за видео надзор је прошао потребну обуку за рад на платформи.

Дефиниција радњи обраде и контекста

Табела 1. Радње обраде видео надзора

Опис радње обраде	Видео надзор
Обрађивани подаци о личности	Слике и видео снимци лица (студенти, запослени, посетиоци)
Намена обраде	Физичка заштита запослених, посетилаца и имовине
Лица на која се подаци односе	Студенти, запослени, посетиоци
Средства обраде	ИКТ за видео надзор
Примаоци личних података	Интерни
Обрађивачи података о личности	Интерно запослени

Нежељени догађаји, који могу настати при радњи обраде видео надзора, могу настати због:

- Мреже и мрежних уређаја
- Процеса/процедура за обраду података о личности
- Запослених који су укључени у обраду личних података
- Обраде личних података у продукционом сектору Академије

Последице, које могу настати при радњи обраде видео надзора, могу бити по:

- Губитак поверљивости
- Губитак интегритета
- Губитак расположивости

Методологија процене ризика

Према стандарду које уређује друштвену безбедност – процену ризика у заштити лица, имовине и пословања СРПС А.Л2.003, ризик се дефинише као „комбинација вероватноће догађаја и његове последице“. Другим речима, ризик је могуће схватити као резултат производа вероватноће догађаја и последица које на основу њега настају и одређује га према наредном обрасцу:

$$P = V \times \Pi$$

где је P – ризик, производ V – вероватноће догађаја и Π – последице догађаја и овако дефинисан ризик у ствари представља очекивање. Вероватноћу је најлакше схватити као одређени степен извесности да ће се одређени догађај десити.

Процена ризика представља системски приступ сагледавању и анализи фактора који утичу на безбедност штићених вредности субјекта

Методологија спровођења поступка процене ризика представља алгоритам, алате и начин спровођења поступка процене, а процедура спровођења поступка процене ризика дефинише стандардизовани низ корака које обезбеђује спровођење поступка у складу са препорукама одговарајућих закона, прописа.

Табела 2. Квалитативни опис вероватноће и квантитативни ранг

Бројчана вредност вероватноће	Квалитативни опис вероватноће	Квантитативни ранг вероватноће
1,2	Занемарљива	1
3,4,5	Мала	2
6,8,9	Средња	3
10,12,15,16	Велика	4
	Изразито велика	5

На основу описа последице и квалитативног описа тежине последице приказан је квантитативни ранг тежине могуће последице

Табела 3. Квалитативни опис последице и квантитативни ранг

Опис последице	Квалитативни опис тежине последице	Квантитативни ранг тежине последице
Нема опасности за живот штитееног лица, безначајна угрожавање имовине и пословања због којих настају проблеми у функционисању који се решавају у склопу редовних активности.	Врло лака	1
Нема опасности за живот штитееног лица, већ лако оштећење. Лако угрожавање имовине и пословања због којих су могући поремећаји у процесу рада.	Лака	2
Потенцијална опасност за живот штитееног лица, значајно оштећење органа али без компликација. Угрожавање имовине и пословања које дозвољава функционисање уз повећане напоре и допунска средства	Средње тешка	3
Стварна опасност за живот штитееног лица, трајно оштећење или уништење органа. Угрожавање имовине и пословања због којег долази до озбиљног нарушавања функционисања организације.	Тешка	4
Смрт штитееног лица, угрожавање имовине и пословања до теме да долази до потпуног прекида функционисања организације.		5

Табела 4. Рангирање ризика

Бројчана вредност ризика	Квалитативни опис ризика	Квантитативни ранг ризик
1,2	Безначајан	1
3,4,5	Мали	2
6,8,9	Средњи	3
10,12,15,16	Висок	4
	Екстремни	5

Вероватноћа догађаја

Мрежа и мрежни уређаји- Ова вероватноћа се процењује као занемарљива јер систем није везан на интернет и није могућ приступ систему са Интернета, а неовлашћен приступ је регулисан контролом овлашћења приступа запослених.

Процеси/процедуре за обраду података личности- настанак овог догађаја се процењује као занемарљив јер су улоге и одговорности оператера за контролу физичког приступа јасно дефинисане, а обрада података о личности се врши у просторијама Академије,

Запослени укључени у обраду личних података- вероватноћа се се процењује као занемарљива пошто се подаци преносе, складиште и обрађују у просторијама Академије док је прихватљива употреба мреже, система и физичких ресурса у Академији јасно дефинисана.

Обрада личних података у продукционом сектору Академије- настанак догађаја процењује се као занемарљив, пошто овај сектор није подложен сајбер нападима, а нема података о пробоју личних података запослених и обрада не укључује велики број лица.

Вероватноћа настанка нежељеног догађаја			
Мрежа и мрежни уређаји	Процеси/процедуре за обраду података личности	Запослени укључени у обраду личних података	Обрада личних података у продукционом сектору Академије
Занемарљива (1)	Занемарљива (1)	Занемарљива (1)	Занемарљива (1)
Укупна вероватноћа настанка нежељеног догађаја			Занемарљива (1)

Упунан резултат евалуације вероватноће догађаја се процењује као **ЗАНЕМАРЉИВ** што представља квантитивни ранг вероватноће 1.

Последице догађаја

Губитак поверљивости- у оквиру специфичне радње обраде последица од губитка поверљивости процењује се да је лака, пошто лице може имати незнатне непријатности, ако се на пример нежељено открије присуство лица у просторијама Академије.

Губитак интегритета- губитак интегритета и расположивости се тешко може догодити са техничког аспекта пошто захтева манипулацију видео слика, па се процењује као лака.

Губитак расположивости- губитак делимичне или потпуне расположивости има низак утицај на лица па се и он сматра лаком последицом.

Последице настанка нежељеног догађаја	Квантитативни ранг тежине последице
Губитак поверљивости	Лака (2)
Губитак интегритета	Лака (2)
Губитак расположивости	Лака (2)
Укупна процена последица настанка нежељеног догађаја	Лака (2)

Упунан резултат евалуације последице нежељеног догађаја се процењује као **ЛАК** што представља квантитивни ранг тежине последице 2.

Евалуација ризика

$$P = B \times \Pi$$

$$P = 1 \times 2 = 2$$

Рангирање ризика

Бројчана вредност ризика	2
Квалитативни опис ризика	Безначајан
Квантитативни ранг ризика	1

Урађеном проценом ризика, закључује се да ризик радњи обраде видео надзора припада рангу 1 што је прихватљив ризик.

Најбоља пракса заштите је примењена да спречи неовлашћен приступ снимцима камера.

ЛОКАЦИЈЕ ВИДЕО НАДЗОРА У ОБЈЕКТУ АКАДЕМИЈЕ ТЕХНИЧКО-ВАСПИТАЧКИХ СТРУКОВНИХ СТУДИЈА-ОДСЕК НИШ

На основу потребе за повећањем безбедности објекта Академије техничко-васпитачких струковних студија- Одсек Ниш, а у складу са Законом о приватном обезбеђењу ("Сл. гласник РС", бр. 104/2013, 42/2015 и 87/2018), Законом о заштити података о личности ("Сл. гласник РС", бр. 87/2018) и Законом о слободном приступу информацијама од јавног значаја („Сл. гласник РС“ бр 120/2004, 54/2007, 104/2009 и 36/2010), израђује се извештај о локацијама видео надзора објекта.

Објекат Академије је спратности П+2 и у оквиру својих капацитета садржи 3 амфитеатра, 6 учионица, 12 канцеларија, 8 лабораторија, скриптарницу, кухињу, библиотеку, салу за презентацију и архиву.

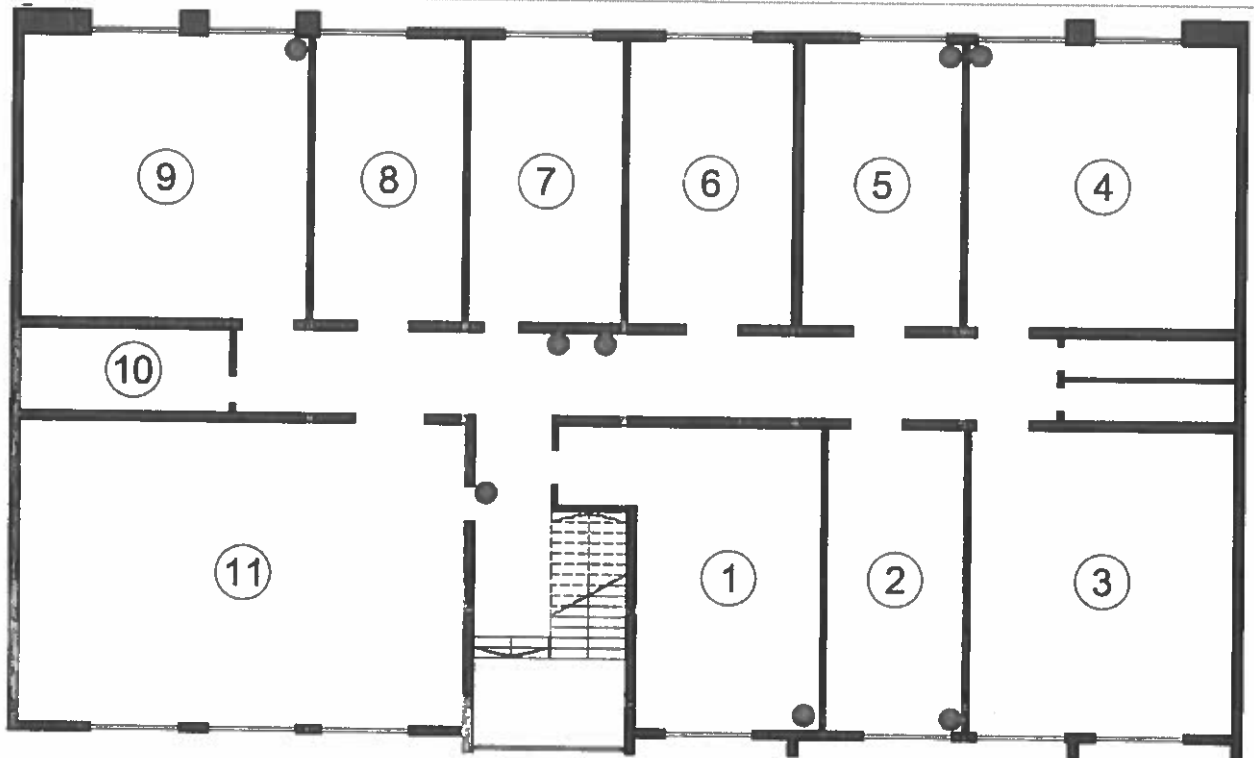
На простору објекта Академије предвиђа се инсталација опреме за видео надзор према члану 29 Закона о приватном обезбеђењу, а у циљу:

- недозвољеног приступа у просторе и објекте који се обезбеђују;
- изношења, односно отуђења и неовлашћеног коришћења штићених предмета;
- уношења оружја, експлозивних, радиоактивних и других опасних предмета и материја;
- провале, диверзије и насилног напада на објекат или одузимање предмета;
- неовлашћеног приступа подацима и документацији;
- других идентификованих ризика.

У складу са наведеним циљевима, распоређивање опреме за видео надзор предвиђа се на следећи начин по етажама:

1. Приземље

Постављање система за видео надзор у приземљу објекта предвиђа се на локацијама које су приказане на слици 1.

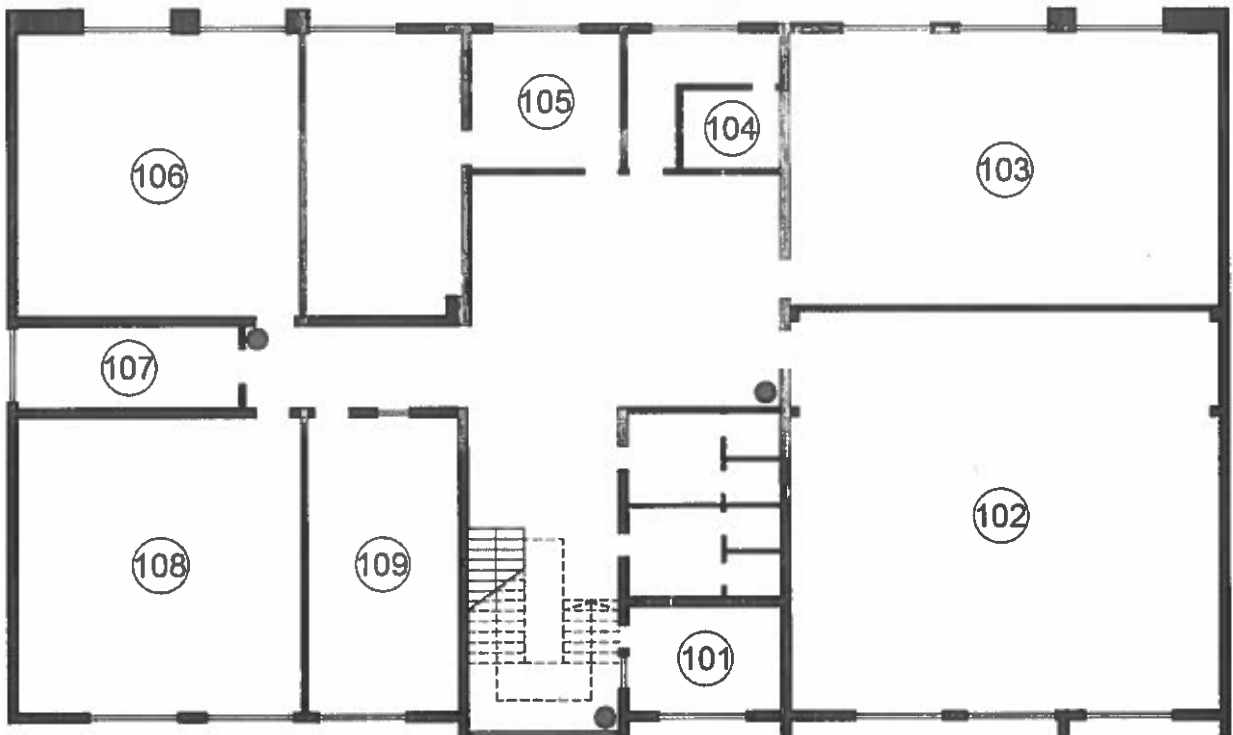


Слика 1. Локације видео надзора на приземљу

- У ходнику приземне етаже предвиђене су три камере. Камера на спољнем зиду изнад просторије број 11 покриваће улаз и излаз са простора објекта. На спољњем зиду просторије 7 предвиђају се две камере тако да свака покрива одређени део ходника. Лево постављена камера покрива улазе у просторије 7,8,9 и 10. Десно постављена камера покрива улазе у просторије 1,2,3,4,5 и 6.
- У просторији 1 (Лабораторија Интернет оф тхингс) поставља се камера због постојања скупоцене опреме за потребе извођења наставе.
- У просторији 2 (Лабораторија МикроТик) поставља се камера због постојања скупоцене опреме за потребе извођења наставе.
- У просторији 5 (Лабораторија за машине и материјале) поставља се камера због постојања скупоцене опреме за потребе извођења наставе.
- У просторији 9 (Лабораторија за заштиту животне средине) поставља се камера због постојања скупоцене опреме за потребе извођења наставе.

2. Први спрат

Постављање система за видео надзор у приземљу објекта предвиђа се на локацијама које су приказане на слици 2.



Слика 2. Локације видео надзора на првом спрату

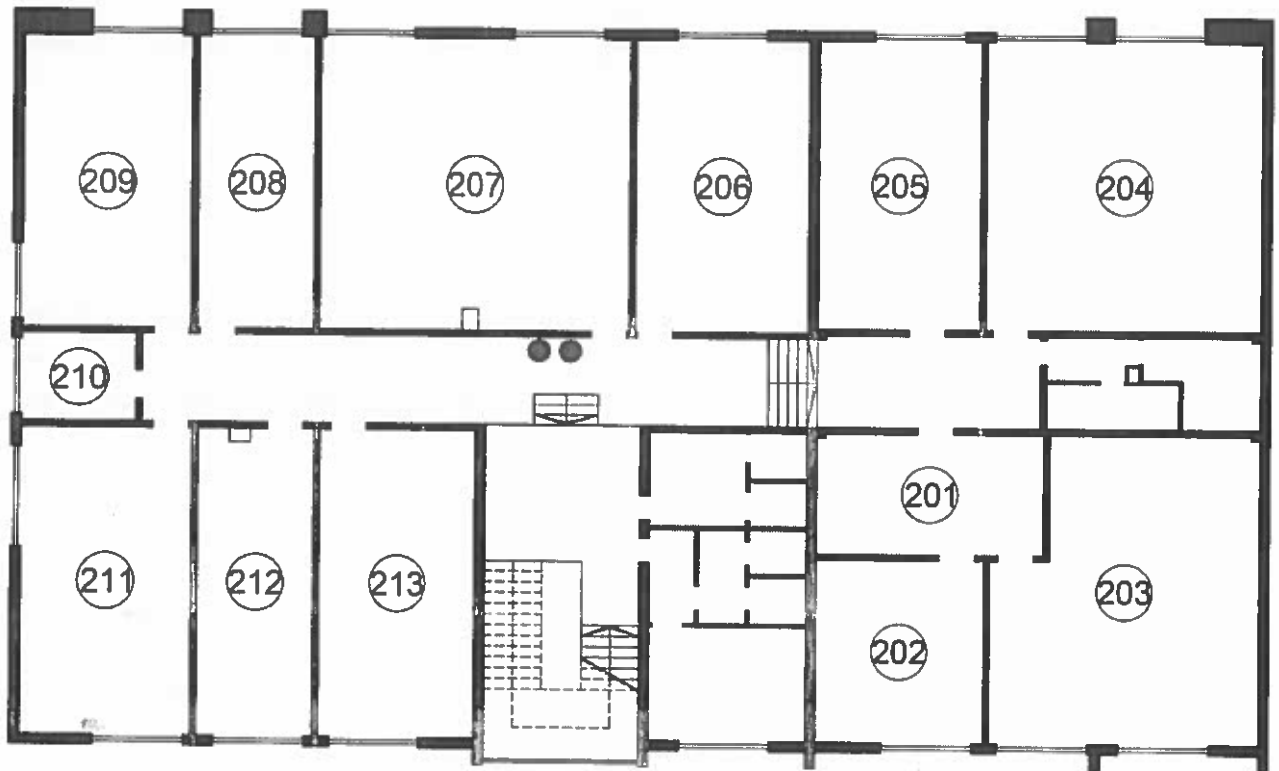
-У ходнику на спољњем зиду просторије 101 (Скриптарница) која поставља се једна камера која обезбеђује степенишни простор и улаз у просторију 101 због постојања школских докумената и инвентара Школе.

-У ходнику на спољњем зиду просторије 107 (Рачуноводство) поставиће се једна камера која покрива улаз у просторије 107, 108 (учионица) и 109 (Студентска служба) због постојања школских докумената и инвентара Школе.

-У ходнику на спољњем зиду просторије 102 (амфитеатар А2) поставиће се једна камера која покрива улазе у амфитеатре А2 и А3, као и 104 (ИТ служба) и 105 (Библиотека) због постојања школских докумената и инвентара Школе.

3. Други спрат

Постављање система за видео надзор у приземљу објекта предвиђа се на локацијама које су приказане на слици 3.



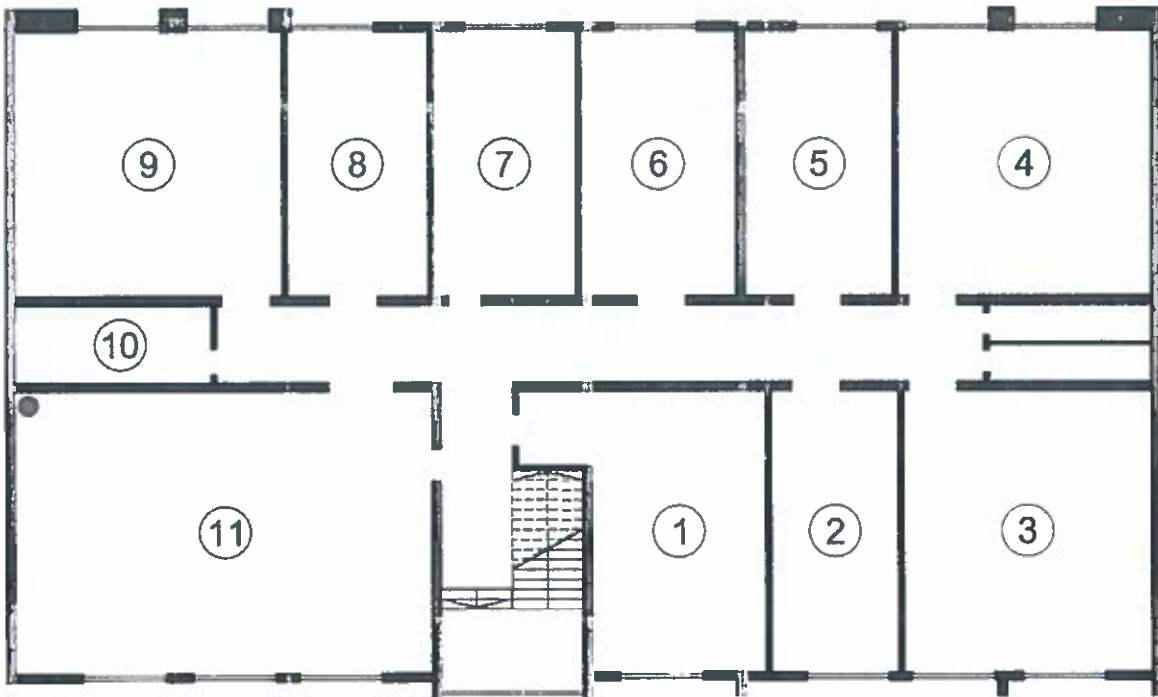
Слика 3. Локације видео надзора на другом спрату

Како се на другом спрату налазе канцеларије у највећем броју, није предвиђен већи број камера. У канцеларијама нису предвиђене камере.

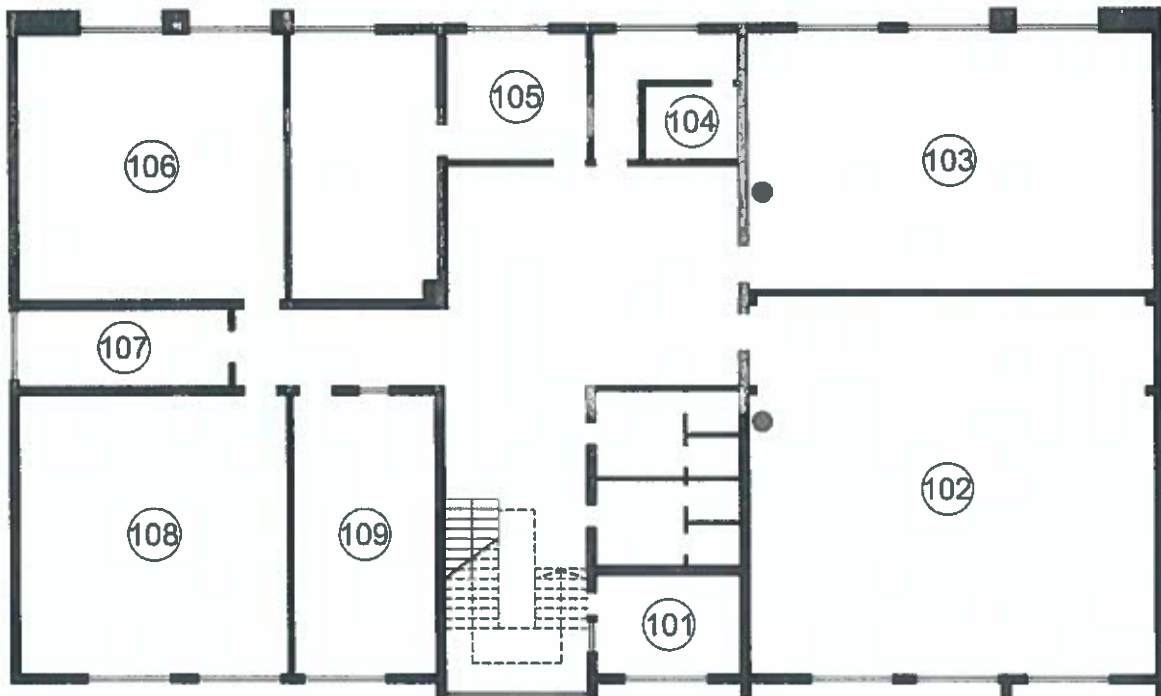
-У ходнику на спољњем зиду просторије 207 поставиће се две камере. Лево постављена камера покрива улазе у просторије 210, 212, 213 (канцеларије), 211 и 209 (лабораторије) и степенишни простор. Десно постављена камера покрива улаз у 204, 206, 207 (учионице), 201 и 205 (канцеларије).

Осим камера које су повезане на систем видео надзора због безбедности објекта, предвиђају се и три камере које ће се налазити ван система видео надзора, а које су постављене у амфитеатрима А1, А2 и А3 (11, 102, 103) са циљем модернизације наставног процеса, спровођења видео конференција, вебинара, одржавања школских свечаности, а све то у оквиру могућности праћења дешавања путем видео линка који би се наменски креирао за сваки догађај посебно.

Позиције камере у свим амфитеатрима дате су на слици 4 и 5. Све камере су усмерене тако да не снимају лица слушалаца, већ су усмерене само ка предавачу, односно простору на коме се одржавају предавања (табла).



Слика 4. Позиција камере у амфитеатру А1 на приземљу



Слика 5. Позиција камере у амфитеатрима А2 и А3 на првом спрату



ЗВЕЗДА припремила
 Јовић Н.