

„NIS2 и киберсигурност. От изискване към устойчивост: NIS2 и новата рамка за киберсигурност в държавните учреждения“

Основни източници: Европейска комисия – NIS2 · Официален текст на Директива (ЕС) 2022/2555 в EUR-Lex · ENISA – NIS2 · ENISA – заплахи срещу публичната администрация

Информацията е съобразена с актуалната рамка на ЕС и данните на ENISA към 2026 г. NIS2 е в сила от 16 януари 2023 г., замени NIS1 от 18 октомври 2024 г. и разширява значително обхвата на европейската рамка за киберсигурност.

От изискване към устойчивост: NIS2 и новата рамка за киберсигурност в държавните учреждения

Дигитализацията на публичния сектор превръща информационните системи в критична инфраструктура за функционирането на държавата. Електронното управление, цифровите регистри, административните услуги и обменът на данни създават значителни ползи, но едновременно с това увеличават зависимостта от сигурността на информационните системи.
NIS2 поставя киберсигурността сред основните управленски приоритети на публичните организации.



Защо киберсигурността е стратегически въпрос?

Съвременната държавна администрация управлява огромни количества информация и предоставя услуги, от които гражданите и организациите зависят ежедневно.
Една успешна кибератака може да доведе до прекъсване на административни услуги, загуба или компрометиране на данни, финансови щети и загуба на обществено доверие.
Затова киберсигурността вече не е само задача на ИТ отделите. Тя е част от управлението на риска и устойчивостта на институцията.



Киберзаплахите срещу публичната администрация

Държавните учреждения са сред най-привлекателните цели за кибератаки поради информацията, която съхраняват, и общественото значение на услугите им.
Сред основните заплахи са:
- ransomware и друг зловреден софтуер;
- фишинг и социално инженерство;
- DDoS атаки;
- кражба на идентификационни данни;
- експлоатиране на софтуерни уязвимости;
- атаки по веригата на доставки;
- кибершпионаж и действия на държавно свързани групи.

Според ENISA публичната администрация остава най-атакуваният сектор в ЕС и представлява около 32% от регистрираните инциденти в Threat Landscape 2026.



Какво представлява NIS2?
NIS2 е европейска директива, чиято основна цел е постигането на високо общо ниво на киберсигурност в Европейския съюз. Тя въвежда общи правила за управление на киберриска, докладване на значими инциденти, надзор и взаимодействие между националните органи.
Рамката обхваща 18 критични сектора, сред които е и публичната администрация.

NIS2 разширява както обхвата на регулираните организации, така и конкретните им отговорности.
Директивата поставя по-силен акцент върху:
управлението на риска → превенцията → реакцията при инциденти → възстановяването → непрекъсваемостта на дейността.
Основната промяна е философска: институцията не трябва просто да има средства за защита, а да бъде способна да предвижда, издържа, реагира и да се възстановява от киберинциденти.



Управление на киберриска

В основата на NIS2 стои подходът, основан на риска. Институциите трябва да идентифицират критичните си активи и услуги, да анализират потенциалните заплахи и уязвимости и да определят възможното въздействие от даден инцидент.
След това трябва да бъдат въведени подходящи и пропорционални организационни, оперативни и технически мерки.
Целта не е премахването на всеки риск, а системното му управление до приемливо ниво.



Човешкият фактор и мерки за сигурност

Дори най-добрата технологична защита може да бъде компрометирана чрез човешка грешка.
Служителите трябва да могат да разпознават фишинг съобщения, подозрителни приложения, опити за социално инженерство и необичайно поведение на информационните системи.
Затова обученията не трябва да бъдат еднократна административна дейност. Необходима е постоянна култура на киберсигурност, при която всеки служител разбира собствената си роля в защитата на институцията.



Управление на уязвимостите

Уязвимостите в софтуера и инфраструктурата са един от основните пътища за проникване в информационните системи.
Ефективната защита изисква:
редовно актуализиране на системите, управление на корекциите за сигурност, наблюдение за нови уязвимости, периодични оценки и тестове на сигурността и ясно определени процедури за отстраняване на откритите слабости. NIS2 поставя управлението и разкриването на уязвимости сред важните елементи на националните и организационните политики за киберсигурност. ENISA



Докладване на значими инциденти

NIS2 въвежда по-структуриран режим за уведомяване при значими киберинциденти.
При определени условия организацията трябва да подаде ранно предупреждение в рамките на 24 часа, последвано от уведомление за инцидента до 72 часа.
След приключване на анализа се предоставя и окончателен доклад, по правило не по-късно от един месец след уведомлението.
Това изисква предварително определени вътрешни процедури – кой установява инцидента, кой го оценява, кой го докладва и кой координира реакцията





Непрекъсваемост и възстановяване

Zero Trust и контрол на достъпа

Ако един Back Up не е тестван не е гаранция за устойчивост

Реакция при киберинцидент

Добрата киберзащита не означава, че инциденти никога няма да възникнат.
Зрялата организация трябва да бъде подготвена да: открие → ограничи → анализира → отстрани → възстанови → извлече поуки.
За тази цел са необходими план за реакция при инциденти, ясно разпределение на отговорностите, комуникационни процедури и периодични симулации на реални сценарии.

Спазването на NIS2 не трябва да се свежда до попълване на документи и изпълнение на формални изисквания. Съответствие означава организацията да покрива определен нормативен минимум.

Киберустойчивост означава организацията реално да може да продължи да функционира в условията на атака, да ограничи последствията и бързо да възстанови критичните си услуги.

Именно преминаването от формално съответствие към реална устойчивост е стратегическата стойност на NIS2.



От съответствие към киберустойчивост

Предизвикателства пред държавните учреждения

остарели информационни системи;
ограничени финансови и човешки ресурси;
недостиг на специалисти по киберсигурност;



сложна и разпределена инфраструктура;
зависимост от външни доставчици;
различно ниво на киберзрялост между институциите;
необходимост от промяна на организационната култура.

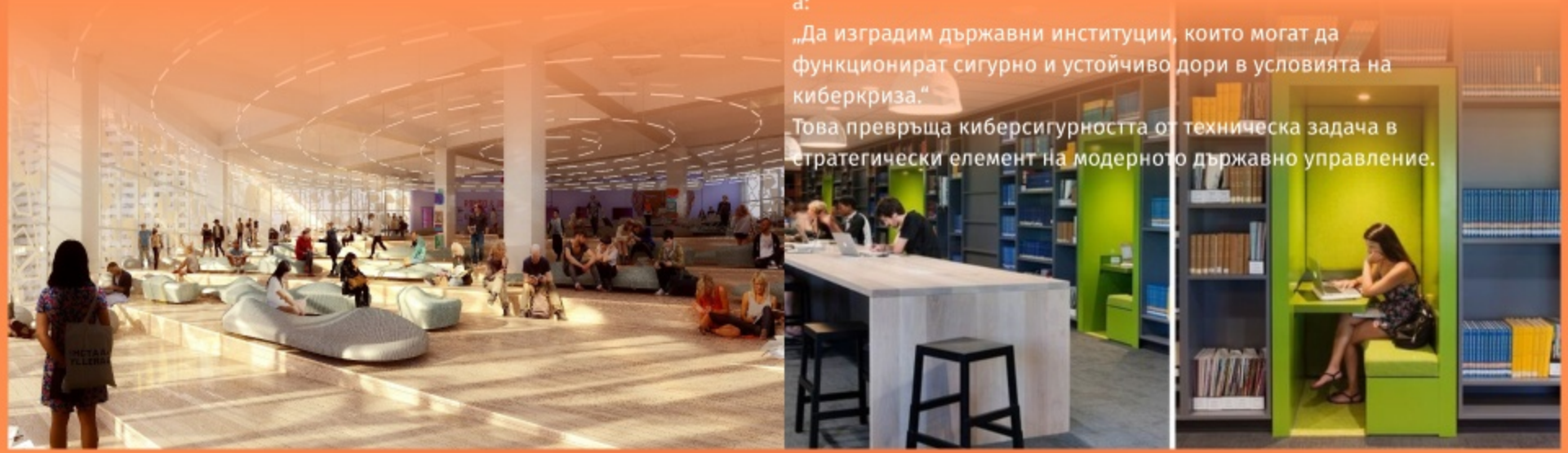


ENISA посочва именно различната зрялост и недостатъчния натрупан опит като важни предизвикателства пред публичната администрация.



NIS2 в българския контекст
За България NIS2 означава развитие на националната нормативна и институционална рамка за киберсигурност и адаптиране на засегнатите публични организации към по-високите европейски изисквания.

Заключение – сигурността като постоянен процес
NIS2 не трябва да бъде разглеждана единствено като още едно регулаторно задължение. Тя поставя основата за промяна в начина, по който публичните институции разбират и управляват киберриска.
Устойчивата държавна организация трябва да може да предвижда заплахите, да защитава системите си, да открива атаките, да реагира своевременно и да възстановява услугите си.
Крайната цел не е просто:
„Да изпълним NIS2."
а:
„Да изградим държавни институции, които могат да функционират сигурно и устойчиво дори в условията на киберкриза."
Това превръща киберсигурността от техническа задача в стратегически елемент на модерното държавно управление.





„NIS2 и киберсигурност. От изискване към устойчивост: NIS2 и новата рамка за киберсигурност в държавните учреждения“

Основни източници: Европейска комисия – NIS2 · Официален текст на Директива (ЕС) 2022/2555 в EUR-Lex · ENISA – NIS2 · ENISA – заплахи срещу публичната администрация

Информацията е съобразена с актуалната рамка на ЕС и данните на ENISA към 2026 г. NIS2 е в сила от 16 януари 2023 г., замени NIS1 от 18 октомври 2024 г. и разширява значително обхвата на европейската рамка за киберсигурност.