



Velox

Сигурна ИТ
инфраструктура

ПОРЕДИЦА NIS2 · КНИЖКА 1 ОТ 3

NIS2

Какво трябва да знае всеки
ръководител за новите европейски
правила за киберсигурност

1 · NIS2

2 · Наръчник по
внедряване

3 · Действие при
инцидент

Съдържание

01	Защо NIS2 засяга и вашия бизнес	3
02	Попада ли организацията ви в обхвата?	5
03	Десетте задължителни мерки с един поглед	8
04	Техническите мерки на практика	10
05	Отговорността на ръководството	15
06	Инциденти: какво и кога се докладва	16
07	Надзор и санкции	18
08	NIS2 в България	19
09	Какво да направите сега	21
—	Речник на термините	22
—	Източници	23
—	Как Велокс може да помогне	24

За тази книжка

Кратко въведение за управители и собственици. Следващите книжки от поредицата описват как се внедряват мерките и какво се прави при инцидент.

Защо NIS2 засяга и вашия бизнес

Кибератаките отдавна не засягат само банките и големите корпорации. Атаки с рансъмуер спират производства, болници и общински услуги, а нападателите често влизат през по-малък доставчик с по-слаба защита.

Какво е NIS2

Директива (ЕС) 2022/2555, известна като NIS2, е общото европейско правило за киберсигурност на организациите, от които зависят икономиката и обществото. Тя замени първата директива NIS от 2016 г. и значително разшири кръга на задължените организации.

Държавите членки трябваше да я въведат в законите си до 17 октомври 2024 г. В България това става с изменения в Закона за киберсигурност, приети в началото на 2026 г.

18

сектора в обхвата

10

задължителни
мерки

24 ч

за първото
уведомление

Какво се променя спрямо първата директива

01 Много повече сектори

Освен енергетика, транспорт и банки, вече са включени храни, отпадъци, производство, куриерски услуги и др.

02 Ясен праг по размер

По правило в обхвата са всички средни и големи предприятия в тези сектори.

03 Еднакви минимални мерки

Десет мерки за управление на риска, задължителни в целия ЕС.

04 Кратки срокове за докладване

24 часа, 72 часа и 1 месец за значителните инциденти.

05 Отговорност и по-високи глоби

Ръководството отговаря лично, а глобите стигат до €10 млн. или 2% от световния оборот.

ОСНОВНОТО ПОСЛАНИЕ

Киберсигурността вече е задължение на ръководството, не само на ИТ отдела.
Управителите одобряват мерките, следят изпълнението им и преминават обучение.

Попада ли организацията ви в обхвата?

Първата стъпка е да разберете дали NIS2 се отнася пряко за вас. Отговорете на три въпроса:

1 В кой сектор работите?

18 сектора в две приложения (стр. 6).

2 Колко е голяма организацията?

По правило средни и големи предприятия.

3 Важи ли за вас изключение?

Някои са в обхвата при всякакъв размер.

Кое предприятие е средно или голямо

Средно

от 50 служители, или оборот и баланс над €10 млн.

Голямо

от 250 служители, или оборот над €50 млн. и баланс над €43 млн.

Броят се и свързаните и партньорските предприятия, например в рамките на група.

В обхвата независимо от размера

Доставчици на електронни съобщения, удостоверителни услуги, DNS и домейни от първо ниво; публичната администрация; единствени доставчици на важна услуга; организации, посочени от държавата.

Секторите в обхвата

Сектори с висока критичност

Приложение I · 11 сектора

Енергетика	Транспорт
Банково дело	Инфраструктура на финансовия пазар
Здравеопазване	Питейна вода
Отпадъчни води	Цифрова инфраструктура
Управление на ИКТ услуги (между фирми)	Публична администрация
Космическо пространство	

Други критични сектори

Приложение II · 7 сектора

Пощенски и куриерски услуги

Управление на отпадъците

Производство и дистрибуция на химикали

Производство, преработка и дистрибуция на храни

Производство: медицински изделия, компютри и електроника, електрически съоръжения, машини, автомобили и други превозни средства

Доставчици на цифрови услуги: онлайн платформи за търговия, търсачки, социални мрежи

Научни изследвания

Внимание: важна е реалната дейност, не кодът по КИД в регистъра. Търговец, който сам доставя храни до магазини, може да попадне в сектор „Храни“.

Съществени и важни субекти

Организациите в обхвата се делят на две групи. Разликата е в надзора и в размера на глобите.

	Съществени	Важни
Кои са	Големите предприятия от Приложение I и някои организации независимо от размера	Останалите в обхвата: средните от Приложение I и всички от Приложение II
Надзор	Превантивен: проверки и одити по всяко време	Последващ: при сигнал или инцидент
Глоба до	€10 млн. или 2% от световния оборот	€7 млн. или 1,4% от световния оборот

Мерките и сроковете за докладване са едни и същи за двете групи. В България окончателното определяне е от компетентните органи (вижте глава 8).

НЕ СТЕ В ОБХВАТА? ПРОЧЕТЕТЕ ТОВА

Организациите в обхвата са длъжни да управляват риска от своите доставчици. Ако им предоставяте ИТ, счетоводни, логистични или други услуги, очаквайте въпросници, нови договорни клаузи и изисквания за сигурност. Добрата подготовка е конкурентно предимство.

Десетте задължителни мерки с един поглед

Директивата изисква подходящи и пропорционални технически, оперативни и организационни мерки, съобразени с рисковете и размера на организацията. Групирахме ги за удобство. Буквите съответстват на чл. 21, ал. 2 от директивата.

Организационни мерки

правила, хора, контрол

(а) Политики за риска и сигурността

Писани правила какво се защитава, от какво и кой отговаря.

(е) Оценка на ефективността

Редовна проверка дали мерките наистина работят.

(ж) Киберхигиена и обучение

Основни безопасни навици за всички и редовни обучения.

(и) Сигурност на персонала

Правила при наемане, смяна на длъжност и напускане.

Пропорционалност: малката фирма не се нуждае от решенията на банка, но трябва да покрие всички десет точки в мащаб, който отговаря на риска.

(б) Управление на инциденти

Как инцидентите се откриват, овладяват и докладват.

(в) Непрекъснатост на дейността

Резервни копия, възстановяване след бедствие, кризисно управление.

(г) Сигурност на веригата на доставки

Изисквания към доставчиците и оценка на риска от тях.

(д) Сигурност при покупка, разработка и поддръжка

Включително управление и разкриване на уязвимости.

Технически мерки

(з) Криптография и криптиране

Защита на данните при съхранение и при пренос.

(и) Контрол на достъпа и активите

Всеки има само нужния достъп; знаете какви системи имате.

(й) MFA и защитени комуникации

Многофакторно удостоверяване и защитени връзки, и при извънредни ситуации.

ПОДРОБНО

Техническите мерки на практика са в глава 4. Пълни насоки за всички мерки ще намерите в книжка 2, „Наръчник по внедряване“.

Техническите мерки на практика

Директивата не назовава конкретни продукти. Това са типичните решения, с които мерките се изпълняват, и буквите на мерките, които подкрепят.

Защитна стена от ново поколение (NGFW) (д) (и)

Филтрира трафика по приложения и потребители, спира атаки и зловреден софтуер.

SIEM (б) (е)

Събира и свързва записите от всички системи и открива подозрителна активност.

Наблюдение на системите (б) (в)

Следи наличността и състоянието на сървъри, мрежа и услуги и сигнализира при отказ.

Защита на крайните устройства (EDR) (б) (д)

Открива и спира атаки на компютри и сървъри, не само известни вируси.

Управление на уязвимости и актуализации (д)

Редовно сканиране и навременно затваряне на пробиви.

Управление на достъпа и MFA (и) (й)

Централни акаунти, права по роли, защитен отдалечен достъп (VPN).

Защитени резервни копия (в)

Копия извън основната мрежа, които рансъмуер не може да промени.

Мрежата: първата линия на защита

(д) (и) (й)

Повечето атаки влизат през мрежата: от интернет, през отдалечения достъп или от вече заразено устройство вътре.

Защитна стена от ново поколение (NGFW)

Разпознава приложения и потребители, а не само адреси. Блокира известни атаки (IPS), филтрира опасни сайтове и проверява файловете за зловреден код. Рутерът от интернет доставчика не я замества.

Сегментиране на мрежата

Отделни зони за офиса, сървърите, гостите, камерите и другите IoT устройства, производството. Заразен лаптоп не трябва да вижда счетоводния сървър.

Защитен отдалечен достъп

VPN с многофакторно удостоверяване за всеки потребител. Никакъв отворен отдалечен работен плот (RDP) към интернет.

Безжична мрежа

Отделна мрежа за гости. За служителите: индивидуални акаунти (WPA2/WPA3-Enterprise) вместо обща парола.

МИНИМУМЪТ ЗА МАЛКА ОРГАНИЗАЦИЯ

NGFW с активни абонаменти за защита, поне три мрежови сегмента, VPN с MFA и нито един панел за управление, достъпен от интернет.

Хора и устройства

(б) (и) (й)

Повечето пробиви започват с откраднат акаунт или заразен компютър.

MFA навсякъде

Имейл, VPN, облачни услуги и особено администраторските акаунти. Където е възможно, ползвайте методи, устойчиви на фишинг (приложение с потвърждение или ключ FIDO2), вместо SMS.

Отделни администраторски акаунти

Ежедневната работа е с обикновен акаунт; привилегирваният се ползва само при нужда. Всеки има минималните права за работата си.

Защита на крайните устройства (EDR)

Класическият антивирус вече не стига. EDR следи поведението на компютрите и сървърите, открива непознати атаки и може автоматично да изолира заразено устройство.

Управление на мобилните устройства (MDM)

Криптиране, заключване и дистанционно изтриване на служебните телефони и лаптопи.

Защита на имейла

Филтър срещу фишинг и зловредни файлове, плюс SPF, DKIM и DMARC срещу подправяне на вашия домейн.

МИНИМУМЪТ

MFA за всички услуги, достъпни отвън, EDR на всички компютри и сървъри и никакви администраторски права за ежедневна работа.

Видимост: да знаете какво се случва

(6) (e)

Срокът от 24 часа предполага, че ще разберете за инцидента навреме. Без записи и наблюдение атаките често се откриват седмици по-късно.

Наблюдение на системите

Постоянна проверка на сървъри, мрежови устройства, интернет връзки и резервни копия, със сигнал до отговорния човек при отказ.

Централни записи на събитията (логове)

Записите от защитната стена, сървърите, облачните услуги и акаунтите се събират на едно място, защитени от промяна, и се пазят достатъчно дълго за разследване.

SIEM

Анализира записите и свързва привидно отделни събития: неуспешни влизания, вход от необичайна държава, голям изходящ трафик. Така открива атаки, които отделните системи не виждат.

Сигналите от EDR

Защитата на крайните устройства (предишната страница) подава сигнали към SIEM, така че картината е пълна.

За доставчиците на цифрови и управлявани ИТ услуги Регламент (ЕС) 2024/2690 изрично изисква наблюдение и регистриране на събития.

КОЙ ГЛЕДА СИГНАЛИТЕ?

Инструментите помагат само ако някой реагира. За малките организации най-реалистично е наблюдението да се възложи като управлявана услуга.

Устойчивост: възстановяване след атака

(в) (д) (з)

Правилото 3-2-1-1-0 за резервни копия

3 копия на данните, на 2 различни носителя, 1 извън офиса, 1 неизменимо или офлайн и 0 грешки при тестово възстановяване.

Тествайте възстановяването

Копие, което никога не е възстановявано, е само надежда. Проверявайте редовно, например веднъж на тримесечие.

Знайте своите RTO и RPO

За колко време трябва да върнете всяка система (RTO) и колко данни можете да си позволите да загубите (RPO).

Уязвимости и актуализации

Пълен списък на устройствата и софтуера. Критичните актуализации се инсталират до дни, не месеци, включително на защитната стена и VPN. Редовно сканиране за уязвимости.

Криптиране

Криптирани дискове на лаптопите и мобилните устройства и защитени връзки (TLS) навсякъде.

Технологията сама не е съответствие. Нужни са и политики, отговорни хора и редовен преглед дали всичко работи.

Отговорността на ръководството

NIS2 поставя киберсигурността в ръцете на управителните органи (чл. 20 от директивата). Не може да се прехвърли изцяло на ИТ отдела или на външен доставчик.

Одобрява

мерките за риска

Наблюдава

как се изпълняват

Отговаря

за нарушенията

Задължително обучение

В България членовете на управителните органи преминават обучение по киберсигурност поне веднъж на две години. Те организират и редовно обучение на служителите.

Лична отговорност

При лична вина ръководителите носят глоби от €500 до €5 000. При съществени субекти, ако предписанията на надзора не се изпълняват, е възможна временна забрана за управленски функции.

НА ПРАКТИКА

Киберсигурността е постоянна точка в дневния ред: с решения, бюджет и отчети.

Инциденти: какво и кога се докладва

Кога инцидентът е „значителен“

Когато е причинил или може да причини сериозно прекъсване на услугите или финансови загуби за организацията, или значителни вреди на други лица. Докладват се само значителните инциденти.

Сроковете

Часовникът тръгва от момента, в който сте разбрали за инцидента.

24 ч

Ранно предупреждение

Има ли съмнение за злонамерено действие или за последици в други държави.

72 ч

Уведомление за инцидента

Първоначална оценка: тежест, въздействие, признаци за компрометиране.

**При
поискване**

Междинен доклад

Актуално състояние, ако органът го изиска.

1 мес.

Окончателен доклад

Причина, предприети мерки, трансгранично въздействие.

Къде се докладва

- До секторния екип за реагиране при инциденти (СЕРИКС), по реда на Закона за киберсигурност.
- Ако са засегнати лични данни, отделно и до КЗЛД в срок до 72 часа по GDPR.
- При нужда уведомете и клиентите, засегнати от инцидента.

Първите стъпки при съмнение

- 1 Изолирайте, не изключвайте.** Откачете засегнатите устройства от мрежата, но не ги изключвайте и не трийте нищо.
- 2 Уведомете отговорното лице** и вашия ИТ доставчик.
- 3 Запишете** какво, кога и как сте забелязали.
- 4 Преценете дали е значителен.** Ако е, 24-часовият срок вече тече.
- 5 Не плащайте откуп** и не влизайте в контакт с нападателите без консултация.

ПОДРОБНО

Пълният план с роли, контакти и шаблони за уведомленията е в книжка 3, „Действие при инцидент“.

Надзор и санкции

Надзорните органи могат да правят проверки и одити, да изискват информация и доказателства, да дават задължителни предписания и да оповестяват нарушенията публично.

Глоби за организациите в България

	Съществени	Важни
Максимум	€10 млн. или 2%	€7 млн. или 1,4%
Минимум за нарушение на мерките или докладването	€25 000	€12 500

Процентът е от световния годишен оборот; прилага се по-високата стойност.

- Неизпълнено предписание: €2 500–12 000, а при повторно нарушение €5 000–25 000.
- Лични глоби за ръководителите: €500–5 000 (вижте глава 5).
- При изтичане на лични данни може да последва и санкция по GDPR.

Глобата често не е най-голямата цена. Спрелят бизнес, изгубените данни и доверието на клиентите струват повече.

NIS2 в България

У нас директивата е въведена със Закона за изменение и допълнение на Закона за киберсигурност (ЗКС), обнародван в Държавен вестник, бр. 17 от 13 февруари 2026 г.

Ключови дати

17.02.2026	Изменения в сила; мерките и докладването важат оттогава
01.06.2026	Край на наполовина намалените санкции
17.08.2026	Срок за решение за секторните органи и методика за определяне на субектите
17.10.2026	Срок за обновената наредба за минималните изисквания
17.11.2026	Срок за нова национална стратегия за киберсигурност

Към октомври 2026 г. част от подзаконовите актове все още се очакват. Следете за промени: датите и органите може да се уточнят.

Кой какво прави

Секторни компетентни органи

Определят кои организации са съществени и важни по методика на Министерския съвет и упражняват надзора в своя сектор.

Регистър на субектите

Непубличен, поддържа се на национално ниво. Промени в данните си (наименование, адрес, контакти, IP адреси) съобщавате в срок до две седмици.

Екипи за реагиране (CSIRT)

Секторните екипи (СЕРИКС) приемат докладите за инциденти. Националният екип (НЕРИКС) координира на национално ниво.

КЗЛД

Комисията за защита на личните данни, когато инцидентът засяга лични данни.

НЕ ЧАКАЙТЕ ПИСМО

Задълженията за мерки и докладване вече важат. Ако смятате, че сте в обхвата, започнете подготовката сега, без да чакате уведомление от органа.

Какво да направите сега

Седем стъпки, с които всяка организация може да започне още този месец:

- ☐ **Проверете обхвата.** Сектор, размер, изключения (глава 2).
- ☐ **Определете отговорен човек** и включете темата в дневния ред на ръководството.
- ☐ **Опишете системите и данните си** и направете първа оценка на риска.
- ☐ **Затворете бързите пропуски:** MFA, проверени резервни копия, актуализации (глава 4).
- ☐ **Подгответе план за инциденти** с роли и контакти за 24-часовия срок.
- ☐ **Обучете ръководството и служителите.**
- ☐ **Прегледайте доставчиците** и договорите с тях.

КНИЖКА 2

Наръчник по внедряване

КНИЖКА 3

Действие при инцидент

Речник на термините

Верига на доставки (supply chain) — доставчиците на продукти и услуги, от които зависи организацията.

Важен субект (important entity) — организация в обхвата с последващ надзор и по-ниски максимални глоби.

Значителен инцидент (significant incident) — инцидент със сериозно въздействие върху услугите, финансите или други лица; подлежи на докладване.

Киберхигиена (cyber hygiene) — основни безопасни навици: силни пароли, актуализации, внимание към фишинг.

Компетентен орган (competent authority) — държавният орган, който упражнява надзор в даден сектор.

MFA (multi-factor authentication) — вход с поне два фактора, например парола и код от телефон.

Непрекъснатост на дейността (business continuity) — способността да продължите работа по време и след инцидент.

Ранно предупреждение (early warning) — първото съобщение за значителен инцидент, до 24 часа.

Рансъмуер (ransomware) — зловреден софтуер, който криптира данните и иска откуп.

СЕРИКС / НЕРИКС (CSIRT) — секторен и национален екип за реагиране при инциденти.

Съществен субект (essential entity) — организация в обхвата с превантивен надзор и най-високи глоби.

Управление на риска (risk management) — откриване, оценка и намаляване на рисковете за системите.

Уязвимост (vulnerability) — слабост в система или софтуер, която може да бъде използвана при атака.

Източници

НОРМАТИВНИ АКТОВЕ

Директива (ЕС) 2022/2555 (NIS2), 14 декември 2022 г.
eur-lex.europa.eu/eli/dir/2022/2555/oj

Регламент за изпълнение (ЕС) 2024/2690 на Комисията
eur-lex.europa.eu/eli/reg_impl/2024/2690/oj

Закон за изменение и допълнение на Закона за киберсигурност, ДВ, бр. 17 от 13.02.2026 г.
dv.parliament.bg

ОФИЦИАЛНИ НАСОКИ

Европейска комисия, Директива NIS2
digital-strategy.ec.europa.eu/en/policies/nis2-directive

ENISA, Агенция на ЕС за киберсигурност
www.enisa.europa.eu

Комисия за защита на личните данни
www.cdpd.bg

СТАНДАРТИ

ISO/IEC 27001:2022, Системи за управление на сигурността на информацията
www.iso.org/standard/27001

Информацията е актуална към октомври 2026 г. Книжката е с информационна цел и не е правна консултация. Предстоят подзаконови актове, които може да уточнят изискванията.



Как Велокс може да помогне

Велокс проектира, изгражда и поддържа ИТ инфраструктура за бизнеса. Помагаме на организациите да преминат от „трябва да направим нещо“ към конкретни, работещи мерки.

Оценка на готовността

Обхват, текущо състояние и списък с пропуски.

Технически мерки

NGFW, SIEM, наблюдение на системите, MFA, резервни копия.

Абонаментна поддръжка

Постоянна грижа за системите, актуализации и наблюдение.

За доставчици

Подготовка за изискванията на клиенти в обхвата на NIS2.

СВЪРЖЕТЕ СЕ С НАС

www.velox-systems.com

office@velox-systems.com

ПОРЕДИЦА NIS2

Три кратки книжки за ръководители, които искат да разберат NIS2 и да действат.

- 1 · NIS2
- 2 · Наръчник по внедряване
- 3 · Действие при инцидент



Velox

Сигурна ИТ
инфраструктура

www.velox-systems.com

office@velox-systems.com

© 2026 Велокс ООД. Информационен материал, не е правна консултация.