ЕВРОПЕЙСКИЙ СОЮЗ

ДИРЕКТИВА NIS2

(Директива ЕС 2022/2555)

Меры по достижению высокого общего уровня кибербезопасности в Союзе

Краткое изложение на русском языке для директоров по информационной безопасности и специалистов по соответствию требованиям

Сведения о документе

Поле	Значение
Official Name	Directive (EU) 2022/2555
Adoption Date	14 December 2022
Publication Date	27 December 2022 (OJ L 333/80)
Entry into Force	16 January 2023
National Transposition Deadline	17 October 2024
Repealed Instrument	Directive (EU) 2016/1148 (NIS1)

> Настоящий документ является неофициальным изложением Директивы ЕС NIS2 от 14 декабря 2022 года и не является авторитетным переводом. Для юридически обязывающего толкования обратитесь к официальному тексту: OJ L 333/80, 27.12.2022.

Содержание

1. Общее резюме

Директива NIS2 (Директива ЕС 2022/2555), принятая Европейским парламентом и Советом 14 декабря 2022 года, является базовой горизонтальной директивой ЕС в области кибербезопасности. Она отменяет и заменяет предшествующую директиву NIS1 2016/1148 с 18 октября 2024 года.

По итогам пересмотра было установлено, что, несмотря на вклад NIS1 в повышение уровня киберустойчивости в Союзе, она оказалась недостаточной для противодействия актуальным и будущим угрозам кибербезопасности. NIS2 существенно расширяет сферу применения, вводит единые критерии, усиливает обязательства по управлению рисками и уведомлению об инцидентах, а также предусматривает более действенные механизмы правоприменения.

Пять основ директивы

1. **Расширенный охват**: регулирование распространяется на большее число секторов и компаний.
2. **Ужесточённое управление рисками**: 10 минимальных технических и организационных мер, закреплённых как обязательные в Article 21.
3. **Многоэтапное уведомление об инцидентах**: раннее предупреждение в течение 24 часов, уведомление об инциденте в течение 72 часов, итоговый отчёт в течение 1 месяца.
4. **Ответственность руководящего органа**: высшее руководство может нести личную ответственность.
5. **Действенные санкции**: административные штрафы до 2% от глобального годового оборота или 10 миллионов евро.

2. Цели и правовая основа

Правовой основой директивы является **Статья 114 Договора о функционировании Европейского Союза (TFEU)**, допускающая принятие мер по сближению национального законодательства в целях создания и обеспечения функционирования внутреннего рынка.

Основные цели директивы:

- Устранить значительные расхождения между государствами-членами и установить единые минимальные требования в области кибербезопасности;
- Создать эффективные механизмы трансграничного сотрудничества и обмена информацией;
- Обновить перечень секторов и видов деятельности, подпадающих под требования кибербезопасности, с учётом актуальной угрозы;
- Обеспечить механизмы правоприменения и средства защиты, гарантирующие эффективное выполнение обязательств;
- Укрепить потенциал киберустойчивости операторов критической инфраструктуры и поставщиков цифровых услуг.

Директива применяется без ущерба и в соответствии с законодательством ЕС о защите персональных данных (GDPR, Regulation EU 2016/679) и конфиденциальности электронных коммуникаций (Директива 2002/58/EC).

3. От NIS1 к NIS2: причины принятия нового регулирования

NIS1, вступившая в силу в 2016 году, стала первым горизонтальным нормативным актом ЕС в области кибербезопасности. В ходе пересмотра были выявлены серьёзные различия в реализации директивы государствами-членами: определение сферы применения в значительной мере оставалось на усмотрение национальных органов, что фрагментировало внутренний рынок.

Выявленные недостатки NIS1

Проблемная область	Ситуация при NIS1	Решение в NIS2
Определение сферы применения	На усмотрение государств-членов; значительные расхождения на практике.	Единое правило «порога размера» для всего ЕС (средние и крупные предприятия).
Перечень секторов	Ограниченное число секторов; значительная часть цифровой экономики не охвачена.	Существенно расширенный охват секторов; включены цифровая инфраструктура, государственное управление, космос и др.
Уведомление об инцидентах	Одноэтапное; сроки и содержание различались между государствами-членами.	Многоэтапное уведомление: раннее предупреждение за 24 ч + уведомление за 72 ч + итоговый отчёт за 1 месяц.
Управление рисками	Общие формулировки; конкретные минимальные меры не определены.	Article 21 закрепляет 10 обязательных категорий минимальных мер.
Санкции	Реализованы на очень разных уровнях в разных государствах-членах.	Гармонизированные максимальные штрафы по всему ЕС (10 млн евро / 2% оборота).
Ответственность высшего руководства	Не определена.	Руководящий орган несёт личную ответственность за соответствие требованиям; обязательное обучение.

NIS2 не является обновлением NIS1; это замена, призванная создать **единую гармонизированную и практически применимую систему кибербезопасности** на пространстве Союза.

4. Сфера применения и исключения

Директива в первую очередь распространяется на субъекты, работающие в секторах **Annex I (высококритичные)** или **Annex II (прочие критические)** на территории ЕС и соответствующие критериям не менее среднего предприятия. Согласно Статье 2 Приложения к Рекомендации Комиссии 2003/361/ЕС, средним предприятием считается предприятие с численностью менее 250 сотрудников и годовым оборотом не более 50 миллионов евро (или итогом баланса не более 43 миллионов евро). NIS2 охватывает субъекты, достигающие порога среднего предприятия или превышающие его: практический минимальный порог для подпадающих под действие директивы субъектов составляет 50 сотрудников или 10 миллионов евро оборота (верхняя граница «малого предприятия» по той же Рекомендации).

Субъекты, охватываемые независимо от размера

- Поставщики публичных сетей электронных коммуникаций и поставщики общедоступных услуг электронных коммуникаций;
- Поставщики доверенных услуг (в соответствии с Регламентом eIDAS, EU 910/2014);
- Реестры доменных имён верхнего уровня (TLD) и поставщики услуг DNS;
- Субъекты, являющиеся единственным поставщиком услуги в государстве-члене либо при нарушении работы которых может быть существенно затронута общественная безопасность, здоровье или охрана;
- Все субъекты центрального государственного управления (определённые национально государствами-членами).

Области, исключённые из сферы применения

Публичные субъекты, деятельность которых осуществляется преимущественно в сферах **национальной безопасности, общественной безопасности, обороны или правоохранительной деятельности** (предотвращение, расследование, выявление и преследование уголовных преступлений), исключены из сферы действия директивы. Также исключены дипломатические и консульские представительства государств-членов в третьих странах и доверенные услуги, используемые в закрытых системах.

5. Ключевые определения

Для правильного понимания директивы необходимо чётко уяснить ряд базовых понятий.

Термин	Определение
Сеть и информационная система	Сети электронных коммуникаций, любое устройство или группа устройств, обрабатывающих цифровые данные, а также все цифровые данные, обрабатываемые для эксплуатации, использования, защиты и обслуживания таких сетей и устройств.
Кибербезопасность	Совокупность мероприятий, необходимых для защиты сетей и информационных систем, пользователей и иных лиц от киберугроз.
Инцидент	Событие, нарушающее доступность, подлинность, целостность или конфиденциальность хранимых, передаваемых или обрабатываемых данных либо услуг, предоставляемых посредством или через сети и информационные системы.
Значительный инцидент	Инцидент, вызвавший или способный вызвать серьёзный сбой в деятельности или финансовые потери для соответствующего субъекта, либо затронувший или способный затронуть иных физических или юридических лиц, причинив им значительный материальный или нематериальный ущерб.
Киберугроза	Любое потенциальное обстоятельство, событие или действие, способное нанести ущерб, нарушить работу или иным негативным образом воздействовать на сети и информационные системы.
Значительная киберугроза	Киберугроза, которая по своим техническим характеристикам предположительно способна оказать серьёзное воздействие на сети и информационные системы субъекта, его пользователей или иных лиц, причинив значительный материальный или нематериальный ущерб.
Уязвимость	Слабость, подверженность или дефект продуктов или услуг ИКТ, которые могут быть использованы киберугрозой.
Квазиинцидент	Событие, которое могло нарушить доступность, подлинность, целостность или конфиденциальность данных или услуг, но было успешно предотвращено.
CSIRT	Computer Security Incident Response Team (группа реагирования на компьютерные инциденты) - - техническая группа, ответственная за обработку инцидентов.
ENISA	European Union Agency for Cybersecurity (Агентство ЕС по кибербезопасности), играющее центральную консультативную и вспомогательную роль в реализации директивы.

6. Категории субъектов: существенные и важные субъекты

Директива делит все охватываемые субъекты на две основные категории. Это разграничение определяет порядок применения обязательств и режима надзора и правоприменения.

Критерий	Существенные субъекты	Важные субъекты
Сектор	Annex I, высококритичные секторы	Annex II, прочие критические секторы (а также средние предприятия Annex I)
Размер	Крупные предприятия (250+ сотрудников или оборот 50+ млн евро)	Средние предприятия (от 50 до 249 сотрудников)
Режим надзора	Как превентивный (ex-ante), так и апостериорный (ex-post) надзор	Только апостериорный надзор -- по доказательствам или жалобам
Максимальный административный штраф	10 миллионов евро или 2% от глобального годового оборота (применяется наибольшая величина)	7 миллионов евро или 1,4% от глобального годового оборота (применяется наибольшая величина)
Санкции в отношении высшего руководства	Может быть применён временный запрет на занятие руководящих должностей	Временный запрет на занятие руководящих должностей не применяется

> **Важное примечание:** если субъект был признан «оператором существенных услуг» по NIS1, государство-член вправе признать его непосредственно существенным субъектом по NIS2. Кроме того, все субъекты, признанные «критическими» по Директиве 2022/2557 (CER), автоматически считаются существенными субъектами по NIS2.

7. Охватываемые секторы (Annex I и Annex II)

Annex I, высококритичные секторы

Крупные предприятия в этих секторах являются существенными субъектами; средние предприятия -- важными субъектами.

Сектор	Подсектор / тип субъекта
Энергетика	Электроэнергия (производство, передача, распределение, снабжение); централизованное теплоснабжение/охлаждение; нефть (трубопроводы, добыча, хранение, транспортировка); природный газ; производство, хранение и транспортировка водорода
Транспорт	Воздушный (авиакомпании, аэропорты, управление воздушным движением); железнодорожный (управляющие инфраструктурой, железнодорожные операторы); водный (операторы морского/внутреннего водного транспорта); автомобильный (интеллектуальные транспортные системы, операторы дорог)
Банковское дело	Кредитные организации в соответствии с Регламентом (EU) 575/2013
Инфраструктуры финансового рынка	Торговые площадки (биржи) и центральные контрагенты (CCP)
Здравоохранение	Поставщики медицинских услуг; референс-лаборатории ЕС; субъекты, проводящие НИОКР лекарственных препаратов; производители фармацевтической продукции; производители медицинских изделий, признанных критическими при чрезвычайных ситуациях в области здравоохранения (согласно Regulation (EU) 2022/123)
Питьевое водоснабжение	Поставщики и распределители воды для потребления человеком
Водоотведение	Субъекты, осуществляющие сбор, удаление или очистку городских, бытовых или промышленных сточных вод
Цифровая инфраструктура	Точки обмена трафиком (IXP); поставщики услуг DNS (за исключением корневых DNS); реестры TLD; поставщики облачных вычислений; поставщики услуг центров обработки данных; поставщики сетей доставки контента (CDN); поставщики доверенных услуг; поставщики публичных сетей/услуг электронных коммуникаций
Управление ИКТ-услугами (B2B)	Managed service providers (MSP); Managed security service providers (MSSP)
Государственное управление	Субъекты центрального и регионального государственного управления, определённые государствами-членами
Космос	Операторы наземной инфраструктуры, эксплуатируемой государствами-членами или частным сектором

Annex II, прочие критические секторы

Сектор	Подсектор / тип субъекта
Почтовые и курьерские услуги	Поставщики почтовых услуг (включая курьерские службы)
Управление отходами	Субъекты, оказывающие услуги по сбору, переработке и утилизации отходов
Химическая промышленность	Субъекты, занимающиеся производством, переработкой и распределением химической продукции
Продовольствие	Крупные предприятия, осуществляющие производство, переработку и оптовое распределение продуктов питания
Производство	Медицинские изделия / изделия для диагностики in vitro; компьютерная, электронная и оптическая продукция; электрооборудование; машины и оборудование прочие; автотранспортные средства, прицепы и полуприцепы; прочее производство транспортных средств
Цифровые поставщики	Онлайн-рынки; интернет-поисковики; платформы социальных сетей
Наука и исследования	Исследовательские организации, проводящие исследования в коммерческих целях

8. Обязательства государств-членов

Директива возлагает обязательства как на государства-члены, так и на субъекты частного сектора. Каждое государство-член обязано предпринять следующие шаги.

Национальная стратегия кибербезопасности. Принять национальную стратегию кибербезопасности с чёткими стратегическими целями, приоритетами и системой управления. Стратегия охватывает такие темы, как безопасность цепочки поставок, программы-вымогатели, поддержка МСП, открытый исходный код и активная киберзащита.

Компетентный орган (органы). Назначить или создать один или несколько компетентных органов для обеспечения реализации директивы и надзора за её соблюдением.

Единая точка контакта (SPOC). Назначить единую точку контакта, ответственную за трансграничную координацию на уровне ЕС.

CSIRT. Учредить или назначить один или несколько CSIRT, ответственных за обработку инцидентов, проактивный мониторинг, скоординированное раскрытие уязвимостей и национальное/международное сотрудничество.

Реестр субъектов. Вести, регулярно обновлять и направлять Комиссии перечень существенных и важных субъектов, а также субъектов, предоставляющих услуги по регистрации доменных имён.

Скоординированное раскрытие уязвимостей. Назначить CSIRT координатором; обеспечить правовую ясность для исследователей в области безопасности.

Взаимная помощь. Оказывать взаимную помощь другим государствам-членам при трансграничном надзоре и правоприменении.

Поддержка МСП. Предоставлять консультации, бесплатные инструменты и национальную/региональную точку контакта для малых и микропредприятий.

9. Меры по управлению рисками кибербезопасности (Article 21)

Важнейшим техническим положением директивы является Article 21. В нём перечислены минимальные технические, операционные и организационные меры, которые обязаны реализовать существенные и важные субъекты. Подход основан на **принципе «всех опасностей»**: охватываются не только кибератаки, но и угрозы, связанные с физическим ущербом, стихийными бедствиями, выходом оборудования из строя и человеческими ошибками.

Article 21, десять минимальных мер

№	Мера	Описание
1	Анализ рисков и политики безопасности информационных систем	Анализ всех рисков и письменная разработка общих политик информационной безопасности.
2	Обработка инцидентов	Процессы предотвращения, обнаружения, реагирования на инциденты и восстановления после них.
3	Непрерывность деятельности	Управление резервным копированием, восстановление после аварий и антикризисное управление.
4	Безопасность цепочки поставок	Включая практики безопасности поставщиков; положения о кибербезопасности в контрактах с прямыми поставщиками.
5	Безопасность при приобретении, разработке и обслуживании сетей и информационных систем	Безопасность на протяжении всего жизненного цикла, включая обработку и раскрытие уязвимостей.
6	Оценка эффективности мер	Регулярная оценка эффективности мер управления рисками.
7	Базовые практики киберзащиты и обучение безопасности	Практики кибергигиены и обучение персонала по вопросам безопасности.
8	Криптография и шифрование	Политики применения шифрования; сквозное шифрование там, где это целесообразно.
9	Безопасность персонала, управление доступом и управление активами	Проверка персонала, авторизация и инвентаризация активов.
10	Многофакторная	Многофакторная аутентификация там, где это целесообразно; непрерывная аутентификация;

10. Обязательства по уведомлению об инцидентах (Article 23)

Наиболее значимым операционным нововведением директивы является многоэтапный режим уведомления об инцидентах. Существенные или важные субъекты обязаны сообщать о **значительных инцидентах**, то есть о тех, которые вызвали серьёзный сбой в деятельности, финансовые потери или существенный ущерб для иных лиц, в CSIRT или компетентный орган в следующие сроки.

Этап	Срок	Содержание
Раннее предупреждение	В течение 24 часов с момента получения сведений об инциденте	Подозрение в том, что инцидент вызван незаконными или вредоносными действиями; возможность трансграничного воздействия; базовая информация для информирования CSIRT.
Уведомление об инциденте	В течение 72 часов с момента получения сведений об инциденте	Обновление раннего предупреждения; сведения о серьёзности, последствиях и, при наличии, индикаторах компрометации (IoC).
Промежуточный/ итоговый отчёт	Не позднее 1 месяца после уведомления об инциденте	Подробное описание инцидента, его серьёзности и последствий; тип использованной угрозы; принятые и планируемые меры по снижению рисков; трансграничное воздействие при наличии.
Отчёт о ходе работ	Если инцидент продолжается на момент наступления срока итогового отчёта	Отчёт о текущем состоянии инцидента; итоговый отчёт -- через 1 месяц после завершения обработки инцидента.

Уведомление получателей услуг: при вероятности возникновения значительной киберугрозы субъекты обязаны незамедлительно и безвозмездно уведомить получателей своих услуг о возможных защитных мерах и, при необходимости, о самой угрозе -- на ясном и понятном языке.

Квазиинциденты и добровольное уведомление

Помимо инцидентов, субъекты **вправе добровольно сообщать о квазиинцидентах и значительных киберугрозах** в CSIRT или компетентный орган. Субъекты, не подпадающие под действие директивы, также вправе направлять добровольные уведомления. Добровольное уведомление не влечёт для заявителя дополнительных обязательств.

> **Практическое значение:** требование о раннем предупреждении в течение 24 часов обязывает субъекты заранее разработать план реагирования на киберинциденты и

11. Безопасность цепочки поставок

Большинство крупных кибератак последних лет достигли своих целей через поставщиков и разработчиков программного обеспечения, а не путём прямой атаки на организацию. Поэтому директива ставит риск цепочки поставок в центр обязательств по управлению рисками.

- Субъекты обязаны оценивать **качество, практики безопасности и процессы безопасной разработки** продуктов и услуг своих поставщиков и провайдеров.
- **Требования к кибербезопасности должны быть включены в контракты** с прямыми поставщиками.
- При выборе **managed security service providers (MSSP)** необходимо проявлять особую осторожность: такие провайдеры являются приоритетными целями для злоумышленников.
- Группа сотрудничества совместно с Комиссией и ENISA проводит **скоординированные оценки рисков безопасности** для критических цепочек поставок (как это было сделано для сетей 5G).
- В сферу оценки входят также **нетехнические факторы риска**, в том числе потенциальное неправомерное влияние третьих стран на поставщиков, скрытые уязвимости и бэкдоры, а также зависимость от провайдеров.

12. Ответственность руководящего органа

Директива обеспечивает переход вопросов кибербезопасности из сферы исключительно технических подразделений в **зону прямой ответственности высшего руководства**. Согласно Article 20, руководящие органы существенных и важных субъектов:

- несут ответственность за **утверждение мер управления рисками** в соответствии с Article 21 и надзор за их реализацией;
- могут быть **привлечены к личной ответственности** за нарушение этих обязательств;
- обязаны регулярно проходить обучение по вопросам кибербезопасности для приобретения достаточных знаний и навыков;
- должны содействовать аналогичному обучению своих сотрудников.

> **Важно:** в отношении существенных субъектов компетентный орган вправе потребовать применения **временного запрета на занятие руководящих должностей** к представителям высшего руководства (в том числе на должности генерального директора или законного представителя). Это крайняя мера, применяемая только после исчерпания всех прочих возможностей правоприменения.

13. Структуры сотрудничества на уровне ЕС

Директива регулирует или укрепляет различные структуры, обеспечивающие эффективное сотрудничество государств-членов.

Структура	Функции
Группа сотрудничества	Поддерживает сотрудничество на стратегическом уровне; разрабатывает двухлетние рабочие программы; публикует руководящие документы; проводит скоординированные оценки рисков для критических цепочек поставок.
Сеть CSIRT	Сотрудничество на операционном уровне; обмен информацией об инцидентах; взаимная помощь; совместное реагирование.
EU-CyCLONe	Сеть европейских организаций связи по киберкризисам; обеспечивает взаимодействие технического и политического уровней при крупных инцидентах и кризисах; подготавливает анализ последствий.
ENISA	Создаёт и ведёт европейскую базу данных уязвимостей; оказывает техническую поддержку; разрабатывает руководства; осуществляет мониторинг политик кибергигиены государств-членов.
Механизмы IPCR	Механизмы интегрированного политического реагирования ЕС на кризисные ситуации (Имплементационное решение Совета 2018/1993); управление кризисами на уровне Союза при масштабных кризисах.
Координатор EU-CSIRTs CVD	В каждом государстве-члене назначается CSIRT-координатор для управления трансграничным скоординированным раскрытием уязвимостей.

Сотрудничество с третьими странами: ЕС может заключать международные соглашения с третьими странами или международными организациями в соответствии с Статьёй 218 TFEU. Такие соглашения могут -- при соблюдении интересов Союза и требований защиты данных -- предоставить соответствующим сторонам право участвовать в деятельности Группы сотрудничества, Сети CSIRT или EU-CyCLONe.

14. Надзор и правоприменение

Директива предусматривает различные режимы надзора для двух категорий субъектов. **Существенные субъекты** подлежат как превентивному, так и апостериорному надзору, тогда как **важные субъекты** находятся под надзором только апостериорно -- по доказательствам или жалобам.

Надзорные полномочия компетентных органов

- Проведение выездных проверок и дистанционного надзора;
- Запрос целевых аудитов безопасности (расходы могут быть возложены на субъект);
- Назначение сканирования безопасности;
- Запрос документации, подтверждающей соответствие мерам управления рисками;
- Запрос информации о действиях, которые предположительно нарушают директиву;
- Запрос информации, предполагающей доступ к персональным данным и данным трафика, при необходимости.

Применимые меры правоприменения

- Выдача предупреждений и обязывающих предписаний;
- Предписание о реализации конкретных мер или устранении уязвимостей в установленный срок;
- Предписание о проведении независимого аудита для проверки мер управления рисками;
- Предписание субъектам информировать получателей услуг о характере нарушения;
- Публичные заявления (с раскрытием наименования субъекта и характера нарушения);
- Для существенных субъектов (крайняя мера): временное приостановление сертификатов или разрешений и временный запрет на занятие руководящих должностей;
- Наложение или инициирование наложения административных штрафов.

15. Административные штрафы

Директива устанавливает **гармонизированные на уровне ЕС максимальные пороговые значения** для административных штрафов, применяемых государствами-членами. Эти пороговые значения привязаны к глобальному обороту субъекта -- аналогично GDPR.

Тип субъекта	Максимальная сумма (применяется наибольшая величина)
Существенные субъекты	10 000 000 евро или 2% от глобального годового оборота
Важные субъекты	7 000 000 евро или 1,4% от глобального годового оборота

Факторы, учитываемые при определении штрафов

- Характер, серьёзность и продолжительность нарушения;
- Причинённый материальный или нематериальный ущерб;
- Умышленный или небрежный характер нарушения;
- Принятые меры по предотвращению или снижению ущерба;
- Степень ответственности и наличие предшествующих нарушений;
- Степень сотрудничества с компетентным органом;
- Иные отягчающие или смягчающие обстоятельства.

Штрафы должны быть **соразмерными**, а при их применении необходимо соблюдать основные права, включая право на защиту, презумпцию невиновности и право на эффективное средство правовой защиты. Государства-члены также вправе предусматривать уголовные санкции за нарушения национального законодательства; при этом ни одно лицо не может быть дважды наказано за одно и то же деяние в нарушение принципа **ne bis in idem**.

16. Сроки реализации и переходный период

Дата	Событие
14 декабря 2022	Принятие директивы Европейским парламентом и Советом
27 декабря 2022	Публикация в Официальном журнале ЕС (OJ L 333/80)
16 января 2023	Вступление директивы в силу (через 20 дней после публикации)
17 октября 2024	Срок имплементации директивы государствами-членами в национальное законодательство
18 октября 2024	Начало применения директивы
18 октября 2024	Отмена Директивы (EU) 2016/1148 (NIS1)
17 апреля 2025	Срок направления государствами-членами перечня существенных и важных субъектов в Комиссию
С 17 октября 2027	Периодический пересмотр реализации директивы Комиссией (каждые 36 месяцев)

Важно: NIS2 является директивой и не применяется непосредственно. Каждое государство-член обязано имплементировать директиву в своё национальное законодательство. Следовательно, конкретные обязательства и санкции, применимые к субъекту, определяются национальным актом об имплементации государства-члена, в котором он осуществляет деятельность.

17. Последствия для компаний за пределами ЕС

Несмотря на то что NIS2 является директивой ЕС, она оказывает существенное влияние на компании за пределами ЕС, прежде всего на те, которые обслуживают рынок ЕС или выступают поставщиками критических субъектов, зарегистрированных в ЕС.

Непосредственно затрагиваемые компании за пределами ЕС

- Компании за пределами ЕС -- **поставщики услуг DNS, облачных вычислений, операторы центров обработки данных, провайдеры CDN, управляемые и управляемые охранные сервисные провайдеры, операторы онлайн-рынков, поисковых систем и платформ социальных сетей** -- предлагающие услуги в ЕС, обязаны назначить представителя в ЕС и соблюдать требования директивы;
- Компании за пределами ЕС, имеющие дочерние структуры или филиалы в ЕС, могут подпадать под действие директивы через эти структуры;
- Поставщики за пределами ЕС, предоставляющие продукты или услуги существенным или важным субъектам ЕС, будут подпадать под **договорные требования безопасности цепочки поставок**, устанавливаемые их заказчиками (Article 21(2)(d));
- Managed service providers и managed security service providers за пределами ЕС, обслуживающие цифровую инфраструктуру или финансовые субъекты ЕС, могут непосредственно подпадать под сферу применения.

Косвенные последствия

- Оценки рисков цепочки поставок со стороны заказчиков в ЕС вынуждают поставщиков за пределами ЕС повышать стандарты кибербезопасности;
- Стандарты, введённые директивой (ISO/IEC 27001, руководства ENISA и др.), становятся **де-факто ориентирами** на глобальном рынке;
- Юрисдикции за пределами ЕС всё чаще используют NIS2 как эталон при разработке собственного законодательства в области кибербезопасности.

18. Практическая дорожная карта соответствия (10 шагов)

Приведённая ниже дорожная карта из 10 шагов служит практическим руководством как для компаний, работающих в ЕС, так и для тех, кто стремится добровольно привести свою деятельность в соответствие со стандартами NIS2.

Шаг	Мероприятие
1. Определение сферы применения	Установить, относится ли компания к секторам Annex I или Annex II, соответствует ли критериям размера, и определить её категорию (существенный/важный субъект).
2. Анализ разрывов	Оценить существующую систему управления информационной безопасностью в соответствии с 10 категориями мер Article 21; выявить разрывы.
3. Структура управления	Установить обязанности, линии отчётности и процессы согласования на уровне совета директоров / высшего руководства; ввести регулярную программу обучения.
4. Политики и документация	Разработать или обновить политику информационной безопасности, политику управления рисками, политику реагирования на инциденты, политику допустимого использования и иные документы.
5. Оценка рисков	Провести инвентаризацию активов, анализ угроз и оценку рисков с применением подхода «всех опасностей»; установить критерии приемлемости рисков.
6. Реализация технических средств контроля	Внедрить многофакторную аутентификацию, шифрование, сегментацию сети, архитектуру нулевого доверия, управление журналами, SIEM, EDR/XDR, резервное копирование и решения по восстановлению после аварий.
7. Потенциал реагирования на инциденты	Задокументировать план реагирования на инциденты; распределить роли и обязанности; выстроить коммуникационную процедуру раннего предупреждения в течение 24 часов; провести настольные учения.
8. Управление цепочкой поставок	Провести инвентаризацию поставщиков; классифицировать их по уровню риска; включить положения о кибербезопасности в шаблоны контрактов; проводить периодические аудиты.
9. Обучение и повышение осведомлённости	Проводить ежегодное обучение по кибергигиене для всего персонала; обеспечивать специализированное обучение для руководящего органа; проводить имитационные фишинговые атаки.
10. Непрерывное совершенствование	Проводить внутренние и внешние аудиты; отслеживать ключевые показатели эффективности; учиться на каждом инциденте; ежегодно обновлять оценку рисков; стремиться к сертификации

19. Заключение и оценка

Директива NIS2 существенно повышает базовый уровень кибербезопасности Европейского Союза. Она не только устанавливает технические требования, но и делает кибербезопасность **неотъемлемой частью системы корпоративного управления и операционной деятельности компаний**.

Сильные стороны директивы

- **Широкий охват**: около 18 секторов и более 100 000 субъектов в зоне действия на пространстве ЕС-27;
- **Гармонизация**: равные условия на внутреннем рынке за счёт единых критериев и режима правоприменения по всему ЕС;
- **Акцент на управление**: возложение ответственности на высшее руководство обеспечивает проникновение кибербезопасности на все уровни компании;
- **Акцент на цепочку поставок**: реагирование на реальность, при которой большинство современных атак осуществляется через цепочку поставок;
- **Структуры сотрудничества**: многоуровневая координация на уровне ЕС через Группу сотрудничества, Сеть CSIRT и EU-CyCLONe.

Критика и вызовы

- Задержки и расхождения в имплементации директивы государствами-членами; на практике единообразная реализация по всему ЕС-27 неравномерна;
- Особенно для средних предприятий затраты на обеспечение соответствия требованиям и преодоление разрыва в технических возможностях представляют серьёзную проблему;
- Реализация требования раннего предупреждения в течение 24 часов до достижения достаточного уровня зрелости может привести к поверхностным или ошибочным процессам уведомления;
- Области пересечения с отраслевыми регулированиями (DORA -- финансы; eIDAS -- доверенные услуги; отраслевые авиационные нормы и др.) могут создавать сложности для субъектов.

Общая оценка

NIS2 переосмысливает кибербезопасность, превращая её из технического вопроса в вопрос **непрерывности деятельности, корпоративного управления и доверия клиентов**. Для субъектов, работающих в ЕС или взаимодействующих с ним, соответствие директиве является одновременно правовым обязательством и способом укрепления операционной устойчивости.

Для компаний за пределами ЕС NIS2 формирует новый **де-факто стандарт** для доступа на рынок ЕС и повышает требования к кибербезопасности в глобальном масштабе. Раннее обеспечение соответствия облегчает выполнение договорных обязательств и повышает общую киберустойчивость.

> **Заключительное примечание:** настоящий документ представляет собой изложение основных положений директивы. Для выявления требований к соответствию, применимых к вашей организации, изучите официальный текст (OJ L 333/80, 27.12.2022), национальный акт об имплементации государства-члена, в котором вы работаете, и отраслевые нормативные акты; при необходимости привлеките юридических и экспертных консультантов по кибербезопасности.

Источники

- Directive (EU) 2022/2555, EUR-Lex CELEX number 32022L2555
- Official Journal of the EU L 333/80, 27 December 2022
- ENISA, European Union Agency for Cybersecurity (www.enisa.europa.eu)
- European Commission Digital Strategy portal (digital-strategy.ec.europa.eu)

Подробнее о NIS2 от Rediacc

Настоящее резюме описывает структуру и обязательства директивы. Сопутствующие руководства на rediacc.com переводят эти обязательства в конкретные операционные и закупочные решения.

Три сопутствующих руководства

- **Article 21(2)(d) и самостоятельное размещение.** Почему реестр сторонних ИКТ сокращается, когда плоскость данных не покидает вашу инфраструктуру. Для директоров по информационной безопасности и специалистов по закупкам, пересматривающих соглашения об обработке данных в 2026 году.
- **Непрерывная эффективность без формализма.** Article 21(2)(e), (f) и Article 23 в совокупности. Форк с постоянным временем выполнения, делающий еженедельные учения реалистичными, и временная шкала уведомления по Article 23, которую невозможно соблюсти без артефактов судебного уровня. Для руководителей по надёжности и эксплуатации.
- **Структурная стоимость соответствия NIS2.** Пятикомпонентный технологический стек, который средние существенные субъекты тихо собирают, что даёт самостоятельно управляемая плоскость управления и какие статьи расходов остаются вашими в любом случае. Для финансовых директоров и закупщиков, вступающих в новый цикл обновления контрактов.

Где найти руководства

Все три руководства вместе с настоящим резюме в виде загружаемого PDF доступны по адресу:

rediacc.com/resources/nis2-directive-summary

Rediacc OÜ -- зарегистрированная в Эстонии платформа для самостоятельного размещения инфраструктуры (регистрационный код 17363830, НДС EE102920091). Продукт не заменяет программу безопасности; это инструментальный слой, устраняющий риск поставщика на уровне плоскости данных, который традиционные инструменты резервного копирования, восстановления после аварий и тестовых данных не могут устранить. Бесплатный уровень Community и платные уровни от 349 долларов США в месяц.

> Настоящий документ и сопутствующие руководства являются учебными материалами. Для принятия решений о соответствии требованиям, применимых к вашей организации, необходимо обратиться к юридическим консультантам и ознакомиться с национальным актом об имплементации в вашей юрисдикции.