

Фот Юлия Дмитриевна
кандидат технических наук, доцент
Оренбургский государственный аграрный университет
Россия, г. Оренбург

Свинарчук Александр Сергеевич
студент
4 курс, факультет «Информационная безопасность»
Оренбургский государственный аграрный университет
Россия, г. Оренбург

Важов Константин Владимирович
студент
4 курс, факультет «Информационная безопасность»
Институт высоких технологий
Россия, г. Оренбург

РАЗБОР АЛГОРИТМА ЕВРОПЕЙСКОЙ ДИРЕКТИВЫ КИБЕРБЕЗОПАСНОСТИ NIS2

Аннотация: Данная научная статья представляет собой анализ актуальности проблемы информационной безопасности в современном мире. Информационная безопасность становится все более важной и актуальной в свете быстрого развития информационных технологий и увеличения объема и значимости цифровых данных. В статье рассматриваются основные аспекты информационной безопасности в Европейском союзе, а именно их директива NIS 2.

Статья основывается на обзоре современной литературы и исследований в области информационной безопасности. В результате анализа были выявлены основные угрозы, с которыми сталкиваются

организации и граждане, включая киберпреступность, хакерские атаки, вирусы и мошенничество в сети.

Ключевые слова: Информационная безопасность, киберпреступность, информационные технологии, цифровые данные, директива NIS 2, киберугроза, цифровая платформа.

STRENGTHENING CYBERSECURITY RESILIENCE: COLLABORATIVE EFFORTS IN THE NIS2

Annotation: *This scientific article is an analysis of the relevance of the problem of information security in the modern world. Information security is becoming increasingly important and relevant in the light of the rapid development of information technology and the increasing volume and importance of digital data. The article discusses the main aspects of information security in the European Union, namely their NIS 2 directive.*

The article is based on a review of modern literature and research in the field of information security. The analysis revealed the main threats faced by organizations and citizens, including cybercrime, hacker attacks, viruses and online fraud.

Keywords: *Information security, cybercrime, information technology, digital data, NIS 2 directive, cyber threat, digital platform.*

В мире, который становится все более цифровым, кибербезопасность стала важнейшим приоритетом для защиты основных услуг и цифровых платформ от киберугроз. Структура Директивы сетевой информационной безопасности 2 (NIS2) , реализованная в Европейском Союзе, представляет собой совместную инициативу с участием различных организаций и органов для повышения устойчивости кибербезопасности.[1]

1. Оценка рисков и определение соответствия [2]:

о Первый шаг во внедрении концепции NIS2 в больнице общего профиля включает проведение комплексной оценки рисков для выявления потенциальных угроз и уязвимостей кибербезопасности. В ходе этой оценки учитывается критическая инфраструктура больницы, информационные системы, медицинское оборудование и данные пациентов, которые могут подвергаться риску. На основании результатов оценки больница оценивает свои меры кибербезопасности и определяет степень соответствия требованиям NIS2.

2. Усовершенствование мер безопасности [3]:

о После определения областей несоблюдения требований и уязвимостей больница внедряет усиленные меры безопасности для укрепления своего положения в области кибербезопасности в соответствии с руководящими принципами NIS2. Сюда входят такие меры, как внедрение контроля доступа, протоколов шифрования, регулярные обновления программного обеспечения, сегментация сети и планирование реагирования на инциденты для эффективного снижения киберрисков.

3. Разработка протокола отчетности об инцидентах и реагирования [4]:

о В больнице установлены протоколы отчетности об инцидентах и реагирования на них, чтобы обеспечить своевременное и эффективное реагирование на инциденты кибербезопасности. Это включает в себя определение ролей и обязанностей, установление каналов связи с соответствующими органами власти и проведение учебных занятий для подготовки персонала к реагированию на инциденты. Протоколы соответствуют требованиям NIS2 по информированию о происшествиях и координации с компетентными органами.

4. Трансграничное сотрудничество и обмен информацией [5]:

о В случае инцидента кибербезопасности с трансграничными последствиями, такого как атака с использованием программы-вымогателя,

затронувшая несколько больниц, больница общего профиля участвует в трансграничном сотрудничестве в соответствии с структурой NIS2. Он сообщает об инциденте национальному компетентному органу и сотрудничает с другими больницами, ENISA и государствами-членами ЕС для обмена информацией об угрозах, координации усилий по реагированию и ограничения последствий атаки через границы.

5. Нормативный надзор и мониторинг соответствия [6]:

препринт

о Регулирующий орган, ответственный за надзор за соблюдением NIS2 в больничном секторе, проводит аудит для оценки соблюдения больницей общего профиля требований кибербезопасности. Регулирующий орган предоставляет рекомендации по устранению любых пробелов в соблюдении требований, контролирует прогресс в реализации мер безопасности в больнице и при необходимости принимает принудительные меры для обеспечения постоянного соответствия стандартам NIS2.

Следуя этому процессу внедрения концепции NIS2 в условиях больниц общего профиля, организации могут повысить устойчивость своей кибербезопасности, защитить критически важные системы здравоохранения и данные, а также внести свой вклад в создание более безопасной экосистемы здравоохранения в Европейском Союзе.

В заключение, концепция Директивы сетевой информационной безопасности 2 (NIS2) предлагает комплексную основу для повышения устойчивости кибербезопасности основных услуг и цифровых платформ в Европейском Союзе. Содействуя более эффективному реагированию на инциденты, расширенному обмену информацией, усилению мер кибербезопасности, трансграничной координации и нормативному надзору, NIS2 стремится смягчить киберугрозы и защитить критически важную инфраструктуру от кибератак. Однако внедрение NIS2 не лишено проблем, включая бремя соблюдения требований, сложность интерпретации,

ограниченность ресурсов, проблемы трансграничной координации и изменчивость правоприменения[7].

В дальнейшем устранение этих ограничений будет иметь решающее значение для оптимизации эффективности NIS2 в повышении устойчивости кибербезопасности. Такие стратегии, как наращивание потенциала и обучение, ясность регулирования и руководство, поддержка распределения ресурсов, стандартизация и гармонизация, а также улучшение трансграничного сотрудничества, могут помочь преодолеть эти проблемы и повысить эффективность NIS2 в эффективной борьбе с киберугрозами. Постоянный диалог, вовлечение заинтересованных сторон и совместные усилия будут иметь важное значение для преодоления этих сложностей и обеспечения постоянного улучшения практики кибербезопасности в ЕС.

Литература

1. Экхардт П. и Котовская А. (2023). Система кибербезопасности ЕС: взаимодействие Закона о киберустойчивости и Директивы NIS 2 // Обзор международного права кибербезопасности, 4(2), 147–164.
2. Эсаяс, С.Ю. (ноябрь 2014 г.). Структурирование идентификации комплаенс-рисков с использованием подхода CORAS // Международный симпозиум IEEE по вопросам обеспечения надежности программного обеспечения (стр. 281–286). IEEE.
3. Рангараджу, С. (2023). Безопасность с помощью интеллекта: улучшение продуктов с помощью мер безопасности на основе искусственного интеллекта. // EPN-Международный журнал науки и техники, 9 (3), 36–41.
4. Рюфл Р., Дорофи А., Манди Д., Хаусхолдер А.Д., Мюррей М. и Перл С.Дж. (2014). Развитие и развитие группы реагирования на инциденты компьютерной безопасности. // Безопасность и конфиденциальность IEEE, 12(5), 16–26.

5. Наваррете, А.С., Меллули, С., Пардо, Т.А. и Хиль-Гарсия, младший (январь 2009 г.). Обмен информацией на национальных границах: расширение полезности теории границ. В 2009 г. // 42-я Гавайская международная конференция по системным наукам (стр. 1–10). IEEE.

6. Робертс, М.К., Фишер, Д.М., Паркер, Л.Е., Дарнелл, Д., Шугарман, Дж., Карритерс, Дж., ... и Зацик, Д. (2020). Этические и нормативные проблемы при прагматическом мониторинге и надзоре за клиническими исследованиями. // Этика и человеческие исследования, 42 (5), 29–37.

7. Шальбрух, М. (2018). Европейская директива по сетевой и информационной безопасности – краеугольный камень единого цифрового рынка. // Открытие цифровых торговых площадок, 287–295