УДК 341.4(4)

В. Г. Пядышев
заведующий кафедрой кибербезопасности
и информационного обеспечения
Одесского государственного университета внутренних дел,
кандидат технических наук, доцент (Украина)

МЕРЫ ЕВРОСОЮЗА ПО УСИЛЕНИЮ КИБЕРБЕЗОПАСНОСТИ

Можно без преувеличения утверждать, что развитие мира сегодня определяется двумя противоречивыми тенденциями, связанными с информатизацией общества, а именно:

- позитивной — усилением компьютерными сетевыми технологиями всех без исключения сфер деятельности человечества;

- негативной: 1) абсолютной зависимостью этих сфер от бесперебойной работы компьютерных сетей; 2) со стремительным развитием различных форм киберпреступности.

Совокупность этих тенденций образует колоссальный фактор риска, что не может не вызывать озабоченности всех стран мира и их содружеств. Не является исключением и Евросоюз, который ведет основательную работу в борьбе за кибербезопасность. Поэтому действия в отношении кибербезопасности, которые осуществляются во всем окружающем мире, целесообразно соотносить с мерами, которые планируются и предпринимаются в Евросоюзе.

Чем определяется в Евросоюзе необходимость по повышению мер кибербезопасности?

Столкнувшись с постоянно растущими вызовами кибербезопасности, ЕС стремится повышать осведомленность о кибератаках, направленных на государства — члены или институты ЕС, а также обеспечивать адекватное реагирование на них.

Мир «Интернет вещей» (IoT) уже стал реальностью, и к 2020 году в ЕС ожидается подключение десятков миллиардов цифровых устройств.

В то же время сегодняшние системы ИКТ могут подвергаться серьезной опасности, такой, как технические сбои и вирусы. Подобные инциденты, часто называемые инцидентами в сетевых и

информационных системах (NIS-инциденты), становятся все более частыми и трудными для решения [1].

Многие предприятия и правительства во всем ЕС для осуществления своих основных функций полагаются на цифровые сети и инфраструктуру. Это означает, что возможные NIS-инциденты могут оказать огромное влияние на компрометацию служб и срыв нормальной работы предприятий.

Кроме того, NIS-инциденты в одной стране могут иметь последствия для других стан и даже для всего ЕС. Случаи нарушения безопасности также подрывают доверие потребителей к онлайн-платежным системам и сетям ИКТ.

Несмотря на растущую угрозу, осознание ее и знания по кибербезопасности по-прежнему недостаточны: 51 % европейских граждан осознают себя неинформированными касательно киберугроз; 69 % компаний не имеют базового понимания о своей подверженности киберрискам.

Итак, 24 октября 2017 года Совет по телекоммуникациям согласился разработать план действий по реформированию системы кибербезопасности ЕС. Министры подчеркнули, что онлайн-безопасность важна для европейских граждан и бизнеса, поскольку ЕС ежегодно теряет около 400 миллиардов евро из-за кибератак.

На чем же предполагается сконцентрировать усилия Евросоюза?

Предлагается общий подход к кибербезопасности ЕС — путь к единому рынку.

В ответ на пакет реформ, предложенный Европейской комиссией в сентябре 2017 года, 19–20 октября 2017 года Совет Европы предложил к принятию общий подход к кибербезопасности ЕС.

По сути, предлагается осуществить реформу на основании мер, установленных в рамках стратегии кибербезопасности, и ее основного компонента — Директивы по безопасности сетевых и информационных систем — директивы NIS (Net Information Systems).

В предложении излагаются новые инициативы:

- создание более сильного агентства кибербезопасности ЕС;
- внедрение схемы сертификации в области кибербезопасности в масштабах всего ЕС;
- оперативное внедрение Директивы NIS.

Лидеры ЕС рассматривают реформу кибербезопасности как один из основных текущих аспектов на пути к созданию Цифрового Единого Рынка ЕС [2, с. 5; 3; 4].

Предлагается создать новое агентство ЕС по кибербезопасности. В своем сентябрьском пакете реформ Европейская комиссия предложила создать более сильное агентство кибербезопасности ЕС на основании структур существующего Агентства по сетевой и информационной безопасности Европейского союза (ENISA). Роль нового агентства будет заключаться в том, чтобы помочь государствам — членам, институтам и предприятиям ЕС противостоять кибератакам [5; 6].

Предлагается схема сертификации по кибербезопасности. Чтобы обеспечить рост рынка кибербезопасности ЕС, Европейская комиссия также предложила внедрить в масштабах ЕС схемы сертификации для продуктов, услуг и процессов в области ИКТ. Они будут оформлены в виде правил, технических требований и процедур. Их роль будет заключаться в снижении фрагментации рынка и устранении регулятивных барьеров, а также в укреплении доверия. Так, например, схемы сертификации будут признаны во всех государствах-членах, что облегчит торговлю через границы [7].

Директива касательно NIS вводится в список приоритетов. Государства-члены должны до 2018 года внести стратегию кибербезопасности в свое национальное законодательство и до декабря 2018 года назначить операторов основных служб.

В мае 2016 года Совет принял общие правила кибербезопасности ЕС. Они вступили в силу в августе 2016 года.

Была введена Директива по сетевой и информационной безопасности (NIS) для расширения сотрудничества между государствами-членами по актуальным проблемам кибербезопасности. Она установила обязательства по безопасности для операторов основных услуг (в таких важных секторах, как энергетика, транспорт, здравоохранение и финансы), а также для поставщиков цифровых услуг (онлайн-рынки, поисковые системы и облачные сервисы).

Согласно директиве NIS, каждой стране ЕС также потребуется назначить один или несколько национальных органов власти и разработать стратегию борьбы с киберугрозами [8; 9].

Предлагаются меры по укреплению Цифрового Единого Рынка. Кибербезопасность может обеспечить инновации и помочь со-

средоточиться на данных как на новой «нефти экономики». Обеспечение безопасного цифрового будущего Европы также может означать:

- устранение угроз онлайн-платформам и предоставление им возможности вносить позитивный вклад в общество;
- поддержку малых и средних предприятий в конкурентной борьбе в цифровой экономике;
- инвестирование в использование искусственного интеллекта и суперкомпьютеров в таких областях, как медицина и энергоэффективность [10].

Дополнительные инициативы. Предложение Европейской комиссии по укреплению кибербезопасности ЕС включает дополнительные инициативы:

- план реагирования на широкомасштабные кибератаки;
- Европейский центр исследований и компетенций в области кибербезопасности с присоединением к нему сети аналогичных центров на уровне государств-членов;
- более эффективный ответ уголовного права на киберпреступность посредством новой Директивы по борьбе с мошенничеством и контрафакцией безналичных платежей;
- укрепление глобальной стабильности через международное сотрудничество [11].

Список основных источников

1. State of the Union 2017 — Cybersecurity: Commission scales up EU's response to cyber-attacks [Electronic resource] // European Commission. Press release. Brussels, 19 September 2017. — Mode of access: http://europa.eu/rapid/press-release_IP-17-3193_en.htm. — Date of access: 02.11.2017.

2. European Council: Conclusions, — 19 October 2017 (EUCO 14/17, CO EUR, 17 CONCL 5). Brussels, 19 October 2017. — 10 p.

3. Resilience, Deterrence and Defence: Building strong cybersecurity in Europe [Electronic resource] / European Commission. 19 September 2017 . — Mode of access: https://ec.europa.eu/digital-single-market/en/news/resilience-deterrence-and-defence-building-strong-cybersecurity-europe. — Date of access: 02.11.2017.

4. Digital single market: Bringing down barriers to unlock online opportunities [Electronic resource] / European Commission . — Mode of access: https://ec.europa.eu/commission/priorities/digital-single-market_en. — Date of access: 02.11.2017.

5. European Union Agency for Network and Information Security [Electronic resource] / Wikipedia, the Free Encyclopedia : site. — Mode of access: https://en.wikipedia.org/wiki/European_Union_Agency_for_Network_and_Information_Security. — Date of access: 02.11.2017.

6. Transport, Telecommunications and Energy Council, 3570th meeting: extracts from the joint press conference by Andrus Ansip, Vice-President of the EC [Electronic resource] / European Commission. 24 October 2017 : site. — Mode of access: https://ec.europa.eu/avservices/video/shotlist.cfm?ref=I145397. — Date of access: 02.11.2017.

7. The EU cybersecurity certification framework [Electronic resource] / European Commission. 13 September 2017 : site. — Mode of access: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework. — Date of access: 02.11.2017.

8. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union // Official Journal of the European Union. — 19.7.2016 (L 194/1). L 194/1- L 194/30.

9. EU-wide cybersecurity rules adopted by the Council [Electronic resource] / Council of the European Union. 17 May 2016. — Mode of access: http://www.consilium.europa.eu/en/press/press-releases/2016/05/17/wide-cybersecurity-rule-adopted/. — Date of access: 02.11.2017.

10. Digital Single Market: Commission calls for swift adoption of key proposals and maps out challenges ahead [Electronic resource] / European Commission. Press release. Brussels, 10 May 2017. — Mode of access: http://europa.eu/rapid/press-release_IP-17-1232_en.htm. — Date of access: 02.11.2017.

11. Commission Recommendation of 13.9.2017 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises. European Commission. Brussels, 13.9.2017. C(2017) 6100 final.