ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ВАГНЕР Евгения Валерьевна

Оценка эффективности и перспективы развития Европейского агентства по сетевой и информационной безопасности (ENISA).
Efficiency evaluation and development perspectives of European Network and Information Security Agency (ENISA).

Выпускная квалификационная бакалаврская работа
по направлению 031900 «Международные отношения»

Научный руководитель –
кандидат политических наук,
доцент кафедры Европейских исследований Д.А. Леви

Студент:_____
Научный руководитель: _____
Работа представлена на кафедру
“___” _____ 2016 г.
Заведующий кафедрой:_____

Санкт-Петербург

2016

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В современном обществе большинство людей знакомы с информационно-коммуникационными технологиями: икт используются дома и на работе, по личным нуждам и для учебы; с их помощью оплачиваются счета, покупаются и продаются вещи, осуществляется взаимодейтсвие с государственными структурами – все это и многое другое проделывается в киберсфере. Но многие ли действительно осознают степень важности и опасности киберугроз? Европейский союз, например, осознает и делает все возможное для того, чтобы обеспечить кибербезопасность хотя бы внутри государств-членов ЕС. Коммерческие предприятия, общество, государственные структуры и национальная безопасность зависят от функционирования информационных технологий и грамотной эксплуатации критически важной информационной инфраструктуры; транспорт, связь, финансовые сервисы, аварийные и коммунальные службы опираются на достоверную, целостную и защищенную информацию, передающуюся через эту инфраструктуру. Именно поэтому для Европейского союза критически значимой является проблема защиты киберпространства. Инцидент, вызывающий нарушение такой инфраструктуры или IT - систем, может привести к серьезным негативным последствиям для функционирования общества и экономики. Для помощи в организации защиты каждого отдельного государства ЕС и Европейского союза в целом было создано агентство по сетевой и информационной безопасности (European Network and Information Security Agency, ENISA), которое должно заниматься быстрым обнаружением, анализом и предотвращением кибер инцидентов, а также мониторингом существующего положения дел с киберугрозами.

ENISA занимается очень широким кругом вопросов: оно создает отчеты о киберугрозах и кибер инцидентах, выпускает полезные материалы для экспертов в области информационных технологий, проводит кибер учения со странами Европейского союза, организациями и гражданами ЕС, взаимодействует с органами и агентствами самого Европейского союза, проводит встречи и конференции и многое другое, однако потенциал своей ENISA еще полностью не раскрыло. Исходя из этого утверждения, данное исследование задалось *целью* дать оценку эффективности и построить сценарий будущего развития агентства. Для достижения этой цели были определены следующие *задачи*:

1. Определить ключевые термины по вопросу киберпространства;

2. Обозначить причины создания, основные цели и задачи агентства по сетевой и информационной безопасности;
3. Рассмотреть и дать оценку эффективности внутренней организации работы ENISA;
4. Обозначить критерии оценки эффективности практической и научной деятельности агентства по сетевой и информационной безопасности;
5. Выявить ключевые факторы для построения прогноза.

Для данного исследования можно выделить две *хронологические рамки* – первые включает в себя время с 2004 года по 2016 в той части работы, которая посвящена истории создания агентства и эволюции его целей, задач и внутренней структуры; вторые включают в себя период с 2014 по 2016 в той части работы, которая посвящена непосредственной деятельности ENISA, поскольку полный пакет документов по итогам года из приближенного к нам времени есть только за 2014 год, за 2015 год есть лишь частичные данные в свободном доступе и за 2016 год в наличии имеется только рабочая программа – полный пакет документов позволит нам просмотреть эффективность работы агентства за 2014 год путем сопоставления планируемых задач и их непосредственного исполнения, а анализ документов за 2015 и 2016 год позволяет просмотреть степень доверия к агентству, его развитие и спрогнозировать возможные перспективы его развития.

Объектом данного исследования является кибербезопасность европейского союза, а *предметом* – европейское агентство по сетевой и информационной безопасности.

Научная новизна заключается в том, что в данном исследовании в научный оборот РФ вводятся новейшие документы агентства до 2016 года включительно. Кроме того, для данного исследования было выведено свое определение «киберпространства», которое, по мнению автора, является наиболее полным отражением всех существующих в нем уровней. Более того, в данном исследовании строится самостоятельный сценарий будущего развития ENISA.

Данная работа основывается преимущественно на источниках по внутренней организации работы агентства и его деятельности. Важнейшим источником является устав агентства по сетевой и информационной безопасности[1]. Вторым по значимости для

1 REGULATION (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No

данного исследования оказалась общеевропейская стратегия кибербезопасности «Открытое, безопасносное и надежное киберпространство»[2], поскольку именно она дает вектор для движения в области обеспечения безопасного киберпространства. Кроме того, важным европейским документом являет конвенция о кибербезопасности, подписанная в 2001 году.[3]

Для данного исследование большое значение оказали внутренние документы ENISA по построению работы, такие как рабочие программы за 2014[4], 2015[5], 2016 год[6], ежегодные отчеты (например, ежегодный общий отчет о работе агентства)[7] и документы финансовой отчетности (например, бюджет агентства на 2014 год)[8].

Важными документами для понимания отношения Европейского союза к кибербезопасности, кроме общеевропейской стратегии и конвенции, оказались

460/2004 [Electronic resource] / / Official Journal of the European Union. 2013. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:JOL_2013_165_R_0041_01&qid=1397226946093&from=EN

2 Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. [Electronic resource] / High Representative of the European Union for Foreign Affairs and Security Policy. Brussel. Feb. 2013 URL: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

3 Convention on cybercrime [Electronic resource] / Council of Europe Budapest. 2001. URL: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (Дата обращения 10.04.2016)

4 Work programme 2014 [Electronic resource] / ENISA. 2013. URL: https://www.enisa.europa.eu/publications/programmes-reports/work-programme-2014 (Дата обращения 10.04.2016)

5 Work Programme 2015 Including Multi-Annual Planning [Electronic resource] / the European Union Agency for Network and Information Security. 2014. URL: https://www.enisa.europa.eu/publications/programmes-reports/enisa-work-programme-2015 (Дата обращения 10.04.2016)

6 Work programme 2016 Including multiannual planning [Electronic resource] / European Union Agency for Network and Information Security. 2015. URL: https://www.enisa.europa.eu/publications/programmes-reports/enisa-work-programme-2016 (Дата обращения 10.04.2016)

7 Annual Activity Report 2014. [Electronic resource] / ENISA. Publications Office of the European Union. 2014. URL: https://www.enisa.europa.eu/publications/programmes-reports/enisa-annual-activity-report-2014 (Дата обращения 10.04.2016)

8 Amending Statement of Estimates no 02/2014 (Amending Budget no 02/2014) [Electronic resource] / European Union Agency for network and information security. 2014. URL: https://www.enisa.europa.eu/about-enisa/accounting-finance/files/annual-budgets/enisa-amending-budget-2-2014 (Дата обращения 10.04.2016)

национальные стратегии по кибербезопасности государств – членов ЕС. Конкретно в данном исследовании использовались финская[9] и испанская[10] стратегии.

Для просмотра эволюции внутреннего устройства агентства по сетевой и информационной безопасности использовались, кроме действующего устава, все прошлые уставы и дополнения к ним за 2004[11] и 2008 года[12].

Помимо этого, для лучшего понимания деятельности агентства использовались новостные источники, преимущественно пресс-релизы ENISA.[13]

Несмотря на то, что основную базу для данного исследования составили источники, в теоретической части использовалась и соотвествующая литература: в основном, общая литература по информационной безопасности[14], обзорные статьи о кибербезопасности[15] и статьи о некоторых проектах ENISA. Особое значение для данной

9 Finland´s Cyber security Strategy [Electronic resource] / Finland. : Forssa print, 2013. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/FinlandsCyberSecurityStrategy.pdf (Дата обращения 10.04.2016)

10 National Cybersecurity Strategy [Electronic resource] / Spain. 2013 URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS_ESen.pdf (Дата обращения 10.04.2016)

11 Regulation (EC) No 460/2004 the European Parliament and of the Council. Establishing the European Network and Information Security Agency [Electronic resource] / Official Journal of the European Union. 2004. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004R0460 (Дата обращения 10.04.2016)

12 Regulation (EC) No 1007/2008 the European Parlament nd of the council of Establishing the European Network and Information Security Agency as regards its duration: amending Regulation (EC) No 460/2004 [Electronic resource] / Official Journal of the European Union. 2008. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2008.293.01.0001.01.ENG (Дата обращения 10.04.2016)

13 New EU Cybersecurity strategy & Directive announced [Electronic resource] / ENISA. 2013. URL: https://www.enisa.europa.eu/media/news-items/new-eu-cybersecurity-strategy-directive-announced (Дата обращения 10.04.2016); New Regulation for EU cybersecurity agency ENISA, with new duties [Electronic resource] / ENISA. 2013. URL: https://www.enisa.europa.eu/media/press-releases/new-regulation-for-eu-cybersecurity-agency-enisa-with-new-duties (Дата обращения 10.04.2016)

14 Панцерев К. А. Современные модели информационного общества: типологическая характеристика // Вестник Санкт-Петербургского университета. Серия 6. Политология. Международные отношения. – 2011. №1.

15 Владимирова Т. В. Об обеспечении информационной безопасности в условиях кибепространства // Вопросы безопасности. – 2014. №3; Добродеев А.Ю., Бородакий Ю. В., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1) // Вопросы

работы имеет научный труд британского социолога Фрэнка Уэбстера[16], а также научная работа преподавателей факультета международных отношений[17] под редакцией Панцерева К.А., доцента кафедры теории и истории международных отношений.

Кроме того, для данного исследования использовалось справочно-энцеклопедическое издание под авторством Воронкова И. М.[18] по терминам в области кибербезопасности.

Методология данного исследования, помимо общенаучных методов таких, как анализ, обобщение, индукция и дедукция, влючает в себя структурно-институциональный метод в вопросах изучения внутреннего устройства агентства, структурно-функциональный метод при определении роли данного агентства для Европейского союза и мирового сообщества, дескриптивный метод при описании агентства и его деятельности, контент-анализ при составлении собственного определения киберпространства и при определении теоретической базы данного исследования и прогностический метод в вопросах перспектив развития агентства в будущем.

Структура исследования включает в себя введение, 3 главы (первые две из которых делятся на 2 параграфа, последняя глава делится на 3 параграфа), заключение, список использованных источников и литературы и приложение. В первом параграфе главы 1 рассматривается теоретическая база данного исследования, во втором параграфе история возникновения агентства и изменение его целей и задач с течением времени. В первом параграфе главы 2 анализируется внутренняя структура агентства, а во втором параграфе экономическая база ENISA. 3 глава посвящена деятельности агентства: в первом параграфе анализируется деятельность агентства в области создания стратегий кибербезопасности, во втором – деятельность внутри Европейского союза, в третьем – международная деятельность. Данная структура позволила широко рассмотреть само агентство и его деятельности и прийти к выводу о его эффективности.

кибербезопасности. – 2013. №1.

16 Уэбстер Ф. Теории информационного общества / М. : Аспект Пресс, 2004.

17 Информационное общество и международные отношения / К. А. Панцерев [и др.], под ред. К.А. Панцирева. – СПб.: изд-во СпбГУ, 2014.

18 Словарь-справочник терминов в области кибербезопасности / авт.-сост. Воронков И.М. и др - М.: Сам полиграфист, 2014. – С. 229

ГЛАВА 1. ВОЗНИКНОВЕНИЕ ЕВРОПЕЙСКОГО АГЕНТСТВА ПО СЕТЕВОЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

1.1 СТАНОВЛЕНИЕ ПОНЯТИЙ «КИБЕРПРОСТРАНСТВО» И «КИБЕРУГРОЗЫ».

Вначале 1990х гг. английский социолог Э. Гидденс предложил теорию «рефлексивной модернизации» общества, основным положением которой является идея о возрастающей организации общества.[19] Модернизация общества предполагает, во-первых, возрастание возможности выбора для всех членов данного общества, который они осуществляют в рамках определенных условий, а во-вторых, рост рефлексивности, которая заключается, согласно Гидденсу, в сборе и обработке информации, необходимой для принятия разного рода решений: «Если сегодня мы выбираем себе религию в соответствии со своими личными убеждениями, то, значит, нам нужна информация о других религиях, чтобы сделать выбор», - пишет Уэбстер.[20] Возникает некая программа: сбор информации, проведение ее анализа, принятие решения на основе возможных рисков. В обществе, где существует подобная схема, всегда будет высокий спрос на информацию, вызванный желанием контролировать ситуацию на всех уровнях — от политического до персонального.

Во-первых, на государственном уровне сбор и обработка информации становятся задачами первостепенной важности, поскольку основными целями государств являются защита собственных границ и национальных интересов, что невозможно без обладания достоверной информацией о существующем положении дел в мире. Для этого возникают сложнейшие системы, которые с помощью специальных компьютерных технологий занимаются непрерывным мониторингом окружающей обстановки во всех сферах жизни общества. Примером может служить американская система Echelon, которая занимается «перлюстрацией электронной почты и факсимильной связи...и хранит в своей памяти 5

19 Уэбстер Ф. Теории информационного общества / М. : Аспект Пресс, 2004. – С. 279

20 Там же 280 с.

трлн страниц текста»[21] (с отсылкой на работу американского писателя и журналиста Джеймса Бэмфорда[22]).

Во-вторых, компьютерные технологии широко используются в военной сфере. В новом информационном обществе изменился тип ведения войн: от индустриального типа к, так называемым, «информационным войнам». Основные отличия нового вида войны заключаются в автоматизации систем управления над рассредоточенными вооруженными силами государства и в «управление восприятием» событий со стороны СМИ (поскольку государству важно преподнести информацию в выгодном для себя свете). Для ведения нового типа войны необходимы самые современные технологии и средства их защиты, тщательное планирование контрударов, чему помогают, например, программируемые системы вооружения, моделирование развития ситуации с помощью компьютерных программ визуализации и системный анализ.[23] Исходя из этого, информационная война является, по факту, заранее запрограммированной, поскольку максимально быстрый ответ на военный акт сможет дать только компьютер, чем и пользуются при ведении данной войны.

В-третьих, использование информационно-коммуникационных технологий применяется в стратегической отрасли экономики, например, использование автоматизированного фрезерного станка в производстве. Все вышесказанное приводит к выводу о том, что киберпространство становится неким новым «полем боя» современных национальных государств.

Кроме того, граждане государств Европейского союза все чаще используют интернет для индивидуальных нужд. Согласно отчету о кибербезопасности[24], 60% граждан стран Евросоюза используют интернет ежедневно для личных нужд (в сравнении с 2013 годом прирост составил 6%[25]) и около 14% используют интернет примерно 5 раз в неделю, а всего лишь 9% не имеют домашнего интернета вообще. В общем, количество

---

21 Уэбстер Ф. Теории информационного общества / М. : Аспект Пресс, 2004. – С. 296

22 Bamford J. Body of secrets: Anatomy of the Ultra-Secret National Security Agency

23 Уэбстер Ф. Теории информационного общества [Текст] / - М. : Аспект Пресс, 2004. – С. 294

24 Cyber Security Report [Electronic resource] : EUROPEAN COMMISSION. 2015. URL: http://ec.europa.eu/COMMFrontOffice/PublicOpinion/index.cfm/Survey/getSurveyDetail/yearFrom/1973/yearTo/2016/search/cyber/surveyKy/2019 (Дата обращения 3.03.2016) p. 9

пользователей интернета (как для личных, так и для рабочих нужд) существенно выросло, а процент людей без доступа к интернету сократился, также снизился процент людей, которые не пользуются интернетом.[26] Кроме того, вырос процент людей, пользующихся социальными сетями, совершающих покупки через интернет и использующих услуги интернет-банка.[27] Данная тенденция роста привела и к возрастанию тревог населения по поводу безопасности в киберпространстве. Согласно отчету, больше всего граждане ЕС беспокоятся о злоупотреблении их персональными данными третьими лицами и о безопасности совершения онлайн операций с денежными средствами. Для того, чтобы обезопасить себя от киберугроз, наиболее популярными методами являются: установка антивируса и игнорирование странного содержания сообщений, присылаемых на почту или в социальных сетях. Однако странным кажется, что лишь 38% людей для своей безопасности стараются не выкладывать персональную информацию о себе в сеть. Хотя это можно объяснить тем, что возрос процент людей, считающих, что именно вебсайты и государство обязаны защищать любую персональную информацию интернет пользователей (таким образом, происходит «перекладывание» ответственности за сохранность данных со своих плеч на чужие).[28] Но стоит отметить, что в данном случае возникает некая «дилемма безопасности»: если государство или организация возьмется за тщательную охрану персональных данных пользователей, то в первую очередь они потребуют полный доступ к любой информации о личности для себя (им необходимо будет знать, что именно защищать). Не приведет ли это к потере свободы? В том и заключается дилемма: для обеспечения высокого уровня защищенности придется жертвовать личной свободой и наоборот. Возможно, что некий процент граждан Европейского союза готовы пожертвовать такой свободой, поскольку процент людей, понимающих опасность киберугроз, все же вырос в среднем на 1,5% по сравнению с прошлым годом,[29] следовательно, люди все больше осознают важность данной сферы.

Таким образом, мы наблюдаем, что киберпространство стало неотъемлемой частью нашего общества — экономика, государственное управление, повседневная жизнь людей и

25 Cyber Security Report [Electronic resource] / European Commission. November 2013. URL: http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf (Дата обращения 3.03.2016)

26 см Приложение 1.

27 см. приложение 2.

28 см. приложение 3

29 см. приложение 4

социальное взаимодействие зависят от правильной работы информационно-коммуникационных технологий. Именно поэтому следует уделять особое внимание защите киберпространства от киберпреступлений различного характера: злоупотреблений частой информацией, вредоносной деятельности, кибертерроризма и т.д. При этом кибербезопасность не может в полной мере осуществляться лишь одной страной и требует международного сотрудничества, поскольку киберсфера не имеет ни государственных, ни каких-либо иных границ. «Кибербезопасность — это глобальная проблема, которая требует глобального ответа» отметила в своем выступлении на Всемирном экономическом форуме в Давосе (2013 г.) Н. Кроес, комиссар ЕС по цифровой политике.[30]

Кибербезопасность стала объектом возрастающего беспокойства и пристального внимания сразу после теракта 11 сентября 2001 г. в Нью-Йорке, когда было установлено, что террористы использовали Интернет для переговоров, разведки, исследования цели и распространения своей пропаганды. Но государства сразу же столкнулись с проблемой, которая мешала и мешает до сих пор плодотворному сотрудничеству – никто не может сформировать единое определение термина «киберпространства» хотя бы на уровне того, считать ли киберпространством только среду Всемирной Сети или в киберпространство включены также различные компьютерные технологии и сети, их соединяющие. Данное исследование смогло сформировать свое понятие киберпространства как трудной для понимания среды, не обладающей физической формой, созданной путем взаимодействия людей, программного обеспечения и Интернета с помощью электричества, специального оборудования и сетей, связанных с ними. Хотя само возникновение термина «cyberspace» приписывают писателю научной фантастики Уильяму Гибсону, который определил киберпространство как «совокупность компьютерных систем, соединенных специальными сетями, с помощью которых происходит коммуникация, хранится и используется электронная информация».[31] Вышеизложенные определения легли в основу понимания киберпространства для данного исследования, а кибербезопасностью будем считать, соответственно, отсутствие угроз в киберпространстве.

Исходя из определения киберпространства, приведенного выше, можно заметить, что киберсфера не является однородной и обладает несколькими уровнями, на которых

30 Kroes N. Speech : EU Cyber Security Strategy. [Electronic resource] / Davos. 24.01.2013 URL: http://europa.eu/rapid/press-release_SPEECH-13-51_en.html (Дата обращения 3.03.2016)

31 Gibson William, Neuromancer (1984)

существует. Дэвид Кларк, американский ученый в области информатики, применил системный подход и вывел те самые «уровни киберпространства»[32]:

1. Физический уровень — то есть физические устройства, являющиеся «фундаментом» киберпространства: это ПК и сервера, «суперкомпьютеры» и энергосистемы, спутники, датчики, а так же иные технические соединители (проводные и беспроводные). Таким образом, на данном уровне киберпространство имеет некоторое географическое расположение и является предметом национальной юрисдикции какого-либо государства;
2. Логический уровень — это код, платформа, обеспечивающая «природу» киберпространства;
3. Информационный уровень — речь идет об информации, которая хранится, передается и преобразуется в киберпространстве;
4. Социальный уровень — люди, которые непосредственно трансформируют натуру киберпространства в результате его использования.

Обладая представлениями о том, что киберпространство является неоднородным и многоуровневым, возникает логичное предположение, что для каждого из этих уровней будут свои киберугрозы, соответственно, для каждого из уровней будут свои собственные, особые, уникальные методы и средства обеспечения безопасности.

Количество кибератак постоянно увеличивается, поскольку все больше граждан и стран вовлечены во взаимодействие через кибернетические сети и программы. В настоящий момент выделяются несколько различных типов классификаций киберугроз, однако исходя из того, что объектом исследования является кибербезопасность Европейского союза, использоваться в данной работе будет классификация из Будапештской конвенции Европейского союза 2001 года, согласно которой угрозы разделяются на[33]:

1. преступления против конфиденциальности, целостности и доступности компьютерных данных и систем (несанкционированный доступ, воздействие на данные, воздействие на функционирование системы и т.д.);

32 Clark D. Characterizing cyberspace: past, present and future. [Electronic resource] / MIT CSAIL. 2010. URL: http://web.mit.edu/ecir/pdf/clark-cyberspace.pdf (Дата обращения 3.03.2016)

33 Convention on Cybercrime [Electronic resource] / Council of Europe. Budapest. 2001. URL: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (Дата обращения 3.03.2016)

2. правонарушения, связанные с использованием компьютерных средств (мошенничество с использованием компьютерных технологий, подделка данных с использованием КТ и т.д.);
3. правонарушения, связанные с содержанием данных (например, распространение детской порнографии);
4. нарушение авторского права и смежных прав

По отношению к объекту киберугрозы могут разделяться на угрозы частным лицам, угрозы организациям и угрозы государству.

Самыми опасными, бесспорно, являются угрозы государственного уровня – это и кибертерроризм (террористические акты с использованием ИКТ, направленные на нарушение работы жизненно важных электронных систем государства, интернет ресурсов и т. д.), и кибервойны (атака одного государства на другое в киберпространстве с целью вывести из строя важные электронные системы), от кибертерроризма отличается субъектами взаимодействия – в случае кибервойны происходит взаимодействие по линии государство-государство, а в случае кибертеррора по линии человек/организация – государство; похищение ценной государственной информации и т. д. В случае успешной атаки, важные государственные информационные системы (например, те, что используют для налогового администрирования) будут выведены из строя, данным из них нельзя будет доверять до тех пор, пока криминалистический анализ не покажет, когда именно произошла атака, как долго система работает на неправильных данных и как можно устранить неполадки. Подобная задержка в работе может нанести ущерб как государству в целом, так и каждому гражданину страны в отдельности[34].

С другой стороны, киберугрозы частным лицам и организациям являются не менее сложными и опасными. Кража личных данных человека, использование его личности преступниками, кража информации об адресах, банковских счетах, кража денег с помощью интернет-банка, взлом аккаунтов в социальных сетях и т.д. — все это может нанести серьезный моральный и финансовый ущерб.

Киберугрозы – это новый вызов для мирового сообщества, трудный в предотвращении и в устранении последствий. Но важнейшим шагом является то, что

34 Jozef Vyskoč, Zsolt Illési, Joanna Świątkowska, Tomáš Rezek Protecting cyberspace in the V4: Towards implementation of the EU's cyber-security strategy [Electronic resource] / Central European Policy Institute Nov. 2013 URL: «http://www.cepolicy.org/publications/protecting-cyberspace-v4-towards-implementation-eus-cyber-security-strategy» (Дата обращения 3.03.2016)

проблема защиты от киберугроз получила признание на государственном уровне. Страны разрабатывают свои собственные организации и агентства для защиты киберпространства (например, в Малайзии существует агентство CyberSecurity Malaysia), стратегии кибербезопасности, законодательную базу для киберсферы – все то, что поможет государству урегулировать данную проблему. Первая стратегия по кибербезопасности была разработана в США в 2003 году (Национальная стратегия о безопасном киберпространстве[35]), после чего Европейский союз также осознал необходимость разработки защиты киберпространства на государственном уровне. Это послужило созданию Агентства по сетевой и информационной безопасности в 2004 году и, впоследствии, разработке общеевропейской стратегии кибербезопасности «Открытое, защищенное и безопасное киберпространство» в феврале 2013 г.[36] На данный момент агентство существует уже 12 лет, поэтому возникает необходимость рассмотреть эффективность данного инструмента Европейского союза и его перспективность.

35 National Strategy to Secure Cyberspace [Electronic resource] / USA. Feb. 2003URL: http://www.dhs.gov/national-strategy-secure-cyberspace (Дата обращения 3.03.2016)

36 Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. [Electronic resource] / High Representative of the European Union for Foreign Affairs and Security Policy. Brussel . Feb. 2013 URL: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf (Дата обращения 3.03.2016)

1.2. ИСТОРИЯ СОЗДАНИЯ АГЕНСТВА ПО СЕТЕВОЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ENISA) И ЕГО ЭВОЛЮЦИЯ.

Устав европейского агентства по сетевой и информационной безопасности был одобрен в марте 2004 года, исполнительный директор назначен в октябре того же года. Агентство было создано с целью регулирования и предотвращения сетевых и информационных угроз, укрепления многостороннего диалога внутри ЕС и за его пределами по данной проблеме, развития культуры сетевой и информационной безопасности в интересах граждан, предприятий и организаций государственного сектора ЕС для способствования нормальному функционированию внутреннего рынка.[37]

Традиционно все европейские агентства должны располагаться в Брюсселе в течение 3 лет до того момента, пока они не будут готовы перебраться в город, в котором они хотели бы базироваться. Однако исполнительный директор и правление ENISA решили перевести агентство сразу же, поэтому данная организация с 1 сентября 2005 года начала свою деятельность в соответствии с регламентом ЕС №460/2004[38] в Ираклионе, Греция, где и располагается на данных момент. Получилось так, что организация начала деятельность раньше, чем были полностью сформированы ее внутренняя структура, что усложнило работу персонала с самого начала деятельности и создало проблемы для формирования рабочей команды.

Первый период существования агентства был трудным из-за царившей неопределенности, так как Великобритания хотела оспорить основание ENISA, апеллируя к тому, что цели данного агентства не соответствуют существующему законодательству Европейского союза в сфере кибербезопасности. Однако, 2 мая 2006 суд постановил, что задачи, возложенные на Агентство статьей 3 устава, соответствуют целям директивы 2002/21 и другим директивам в области сетевой и информационной безопасности.[39] Таким

37 Regulation (EC) No 460/2004 of the European Parliament and of the Council Establishing the European Network and Information Security Agency (Text with EEA relevance) [Electronic resource] / Official Journal of the European Union. 10 March 2004 URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004R0460 (Дата обращения 08.03.2016)

38 Ibid.

39 United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union / Case C-217/04 URL:

образом, несмотря на положительное решение суда, на деятельность агентства была брошена тень, что помешало первой волне набора персонала. К тому же, мандат на деятельность ENISA был выдан только до 2009 года, а значит, агентство могло предлагать контракты, ограниченные во времени, действие которых прекратилось бы, если мандат не был бы продлен, что тоже не способствовало доверию.[40] В 2007 году независимыми экспертами проверочной комиссии в составе Габриэллы Катанео, Эрика Домаг и профессора Джеймса Бэкхауза[41] было проведено глобальное исследование эффективности организации, в результате которого комиссия рекомендовала продлить мандат агентства: «Комиссия рекомендует продление мандата Агентства с поддержанием его существующих целей и проводимой политики…»[42]. Благодаря этому, в 2008 году Европейский парламент и Совет принял Регламент № 1007/2008[43] о продлении мандата Агентства по сетевой и информационной безопасности до марта 2012 года, а в 2011 году регламентом № 580/2011[44] мандат был продлен до 13 сентября 2013 года.

---

http://curia.europa.eu/juris/showPdf.jsf;jsessionid=9ea7d2dc30db8ba88b5908ff47d6961c9f441c2ac18d.e34KaxiLc3qMb40Rch0SaxuKaNr0?docid=57031&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=5545180 (Дата обращения 08.03.2016)

40 Владимирский А. Европейский парламент дает «зеленый свет» Агентству ENISA на реализацию Стратегии кибербезопасности ЕС [Электронный ресурс] / Экспертный центр электронного государства. 2013. URL: http://d-russia.ru/evropejskij-parlament-daet-zelenyj-svet-agentstvu-enisa-na-realizaciyu-strategii-kiberbezopasnosti-es.html (Дата обращения 08.03.2016)

41 Gabriella Cattaneo, expert evaluator and director of of the Expertise Centre on Competitiveness and Innovation Policies and Strategies of IDC and IDC Health Insights EMEA; Eric Domage, IDC EMEA research manager for IT and security; professor James Backhouse, senior lecturer at the Department of Information Systems of the London School of Economics.

42 Evaluation of the European Network and Information Security Agency [Electronic resource] / Final Report. Experts Panel IDC EMEA. URL: http://ec.europa.eu/smart-regulation/evaluation/search/download.do;jsessionid=rpwq5oEp3UR9t_KpFpSEG2Sq2uVnPh0EwEj3aYj2vxrIRun8DRRA!1168777535?documentId=814 (Дата обращения 08.03.2016) p. 13

43 Regulation (EC) No 1007/2008 of the European Parliament and of the Council of Establishing the European Network and Information Security Agency as regards its duration: amending Regulation (EC) No 460/2004 [Electronic resource] / Official Journal of the European Union. 2008 URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2008.293.01.0001.01.ENG (Дата обращения 08.03.2016)

44 Regulation (EU) No 526/2013 of the European Parliament and of the Council concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 [Electronic resource] / Official Journal of the European Union. 2013 URL: http://eur-lex.europa.eu/legal-

18 июня 2013 года европейский парламент одобрил новый, последний регламент, гарантирующий продление мандата агентства на семилетний срок (до 2020 года) с некоторыми расширенными функциями. Исполнительный директор ENISA, профессор Удо Хельбрехт отметил, что с принятием нового регламента ENISA получило больше возможностей для обеспечения безопасного европейского киберпространства, и теперь агентство будет работать в более тесном контакте с государствами-членами Европейского союза и с Европолом для пресечения киберпреступлений.[45] Новый регламент закрепил достижения ENISA в области работы команд быстрого реагирования по компьютерной помощи в государствах-членах ЕС (Computer Emergency Response Teams, CERTs), а также в области проведения международных киберучений, таких как, например, Кибер Европа 2012 года (около 600 участников)[46]. Ключевые изменения регламента включают в себя также: обеспечение тесного взаимодействия агентства по сетевой и информационной безопасности с центром Европола по киберпреступлениям (European Cybercrime Centre, EC3); оказание помощи в разработке европейской политики по кибербезопасности и законодательства в данной сфере; обнаружение и предотвращение трансграничных киберугроз и т.д.[47] Кроме того, с целью повышения эффективности, агентство создало филиал в центральном районе Афин.

content/EN/TXT/HTML/?uri=OJ:JOL_2013_165_R_0041_01&qid=1397226946093&from=EN#ntr6-L_2013165EN.01004101-E0006 (Дата обращения 8.03.2016)

45 New Regulation for EU cybersecurity agency ENISA, with new duties [Electronic resource] / ENISA. 2013 URL: https://www.enisa.europa.eu/media/press-releases/new-regulation-for-eu-cybersecurity-agency-enisa-with-new-duties (Дата обращения 8.03.2016)

46 Cyber Europe 2012 : Key Findings Report [Electronic resource] / ENISA. 2012 URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/cyber-europe-2012/cyber-europe-2012-key-findings-report (Дата обращения 8.03.2016)

47 Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 [Electronic resource] / Official Journal of the European Union. 2013. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:JOL_2013_165_R_0041_01&qid=1397226946093&from=EN (Дата обращения 8.03.2016)

На настоящий момент Агентство по сетевой и информационной безопасности занимается деятельностью на основе последнего регламента 2013 года №526/2013[48]. Согласно данному регламенту, ENISA должно заниматься:

1. сбором информации и данных, необходимых для проведения анализа угроз кибербезопасности;
2. мониторингом состояния сети и информационной безопасности в Европейском союзе совместно с государствами-членами ЕС, Комиссией и заинтересованными сторонами;
3. обеспечением сотрудничества между институтами ЕС, его органами, ведомствами, агентствами и государствами-членами, а также повышением уровня сотрудничества между заинтересованными сторонами в Евросоюзе, в частности, с помощью вовлечения национальных органов, органов ЕС, экспертов из частного сектора в соответствующих областях (например, провайдеров сетей и услуг электронных коммуникаций, поставщиков программного обеспечения);
4. оказанием помощи в проведение диалога институтам ЕС, государствам-членам Евросоюза с индустрией по производству компьютеров и программного обеспечения, тем самым способствуя совместному подходу к предотвращению угроз сетевой и информационной безопасности;
5. содействием развитию политики и законодательства в области кибербезопасности Европейского союза путем проведения консультаций и анализов существующей обстановки, а также обеспечением подготовительной работы для обновления политики и законодательства ЕС в данной сфере;
6. оказанием помощи государствам-членам Евросоюза, его институтам и органам в развитии навыков профилактики, обнаружении и ликвидации угроз сетевой и информационной безопасности, а также в развитии европейской системы раннего предупреждения, который бы дополнял национальные механизмы подобного типа;
7. поддержкой научных исследований, разработок и стандартизации путем содействия созданию европейских и международных стандартов в области управления рисками, а также в области безопасности электронных продуктов, сетей и услуг;

48 Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 [Electronic resource] / Official Journal of the European Union. 2013. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:JOL_2013_165_R_0041_01&qid=1397226946093&from=EN (Дата обращения 8.03.2016)

8. содействием международному сотрудничеству в области сетевой и информационной безопасности путем организации международных учений в области кибербезопасности, содействия международному обмену опытом и т.д.

Обозначенные в уставе ENISA цели и задачи помогут сделать вывод в данном исследовании об эффективности организации, основываясь на том, соответствует ли им нынешняя деятельность агентства.

ГЛАВА 2. ОРГАНИЗАЦИЯ РАБОТЫ АГЕНСТВА ПО СЕТЕВОЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ENISA).

2.1. ВНУТРЕННЯЯ СТРУКТУРА АГЕНТСТВА ПО СЕТЕВОЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЕЕ ВСПОМОГАТЕЛЬНЫЕ ЭЛЕМЕНТЫ.

Для эффективной деятельности организации немалую роль играет то, насколько грамотно организована ее структура – нет ли ненужных элементов или, наоборот, возможно какой-то части агентству не хватает? Именно для этого в данном исследовании разбирается структура ENISA.

Структура агентства по сетевой и информационной безопасности включает в себя такие основные элементы, как:

1. правление (Management Board);
2. исполнительный комитет (Executive Board);
3. Исполнительный Директор (Executive Director) с его сотрудниками;
4. и группу заинтересованных сторон (Permanent Stakeholders' Group).

Также, по требованию, могут создаваться временные рабочие группы, которые включают в себя специалистов в сфере сетевой и информационной безопасности из различных государств – членов Европейского Союза. Разберем каждый элемент и его значение для ENISA подробнее, основываясь на уставе агентства и документах о внутренней организации работы.

Правление по своей сути существует для того, чтобы организовывать работу агентства по сетевой и информационной безопасности в соответствии с правилами, установленными уставом ENISA. К основным задачам данного элемента структуры относятся:

1. Принятие годовых и многолетних планов работы агентства;
2. Предоставление ежегодного отчета о работе ENISA в Европейский парламент, Совет, Комиссию и суд Аудиторов, а также размещение данного отчета на сайте ENISA с целью сделать его публичным;
3. Разрешение конфликтов интересов внутри агентства;

4. Издание правил найма сотрудников;
5. Назначение на должность или освобождение от занимаемой должности Исполнительного Директора агентства;
6. Принятие правил работы для себя и исполнительного комитета после одобрения их Комиссией ЕС;
7. Принятие правил внутренней работы всего агентства;
8. Принятие документов, касающихся финансовых вопросов по работе агентства;
9. Назначение представителей группы заинтересованных сторон.

Правление состоит из одного представителя от каждого государства-члена и 2 представителей от Комиссии. Каждый представитель должен назначить своего заместителя, который будет исполнять его обязанности в его отсутствие. Срок работы правления 4 года. Каждые 3 года правление выбирает Председателя и его Заместителя - этот хороший ход позволяет организовать максимально непредвзятое правление.

Правление проводит обязательную встречу раз в год, но по требованию Председателя или более трех членов правления могут проводиться дополнительные встречи. Решения принимаются абсолютным большинством голосов.

На данный момент Председателем правления является представитель Швеции, заместитель директора отдела по политике в области информационных технологий министерства предпринимательства, энергетики и коммуникации Йорген Самуэльссон.[49]

В помощь себе правление создает исполнительный комитет, который, в основном, подготавливает проекты по административным и финансовым вопросам на обсуждение в правление, а также, кроме этого, помогает Исполнительному Директору в претворении в жизнь решений правления по данным вопросам.

Исполнительный комитет состоит из пяти членов, входящих также в правление, включая Председателя правления (который может стать и Председателем исполнительного комитета) и одного представителя от Комиссии. Встречи проводятся раз в три месяца, но по требованию Председателя могут созываться экстренные встречи. Срок работы исполнительного комитета такой же, как у правления – 4 года.

---

49 List of ENISA Management Board Representatives and Alternates [Electronic resource] / ENISA. URL: https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/MBMemberAlternate.pdf (Дата обращения 16.03.16)

Правление назначает на должность Исполнительного Директора, который является представителем агентства по сетевой и информационной безопасности. Основные задачи Исполнительного Директора включают в себя:

1. Управление ежедневной работой агентства;
2. Претворение в жизнь решений правления;
3. Разработку и воплощение в жизнь проектов работы агентства;
4. Подготовку ежегодного отчета о работе агентства, а также планов работы на будущее;
5. Развитие и поддержание связей агентства с европейскими институтами, органами, агентствами, бизнес организациями и пользователями с помощью своих сотрудников;
6. Создание, по необходимости, специальных временных рабочих групп. Например, временные рабочие группы по оценке и регулированию рисков, которые ENISA создает для повышения уровня культуры безопасности у населения, бизнес-сообщества и государств-членов Европейского союза путем обеспечения высокого уровня сетевой и информационной безопасности.

В начале существования агентства в распоряжении у Исполнительного директора было довольно много персонала. Исполнительный директор обладал личным советником по проведению политики агентства, отделом по связи с общественностью и секретариатом. Кроме того, в его распоряжении находилось три департамента[50]:

1. административный департамент (administration department), в который входили отделы по HR, финансам, юридическому обслуживанию (legal services), информационно-коммуникационным технологиям (ICT Infrastructure) и секретариат;
2. технический департамент (technical department), в который входили отделы по управлению рисками (risk management), технологиям сетевой и информационной безопасности (network and information security technologies), политике для организаций по сетевой и информационной безопасности (network and information security policies for organizations) и секретариат;
3. и департамент по взаимодействию и поддержке (cooperation and support department), в который входили отделы по политике реагирования на

50 General report 2005 [Electronic resource] / ENISA. Brussels. 2005 URL: https://www.enisa.europa.eu/publications/programmes-reports/enisa_work_programme_2005.pdf (Дата обращения 08.03.2016) p. 11

компьютерные инциденты (computer incident and response handling policy), по взаимодействию с органами Европейского союза и его государств-членов (relations with EU bodies and member states), по взаимодействию с производствами и международными институтами (relations with industry and international institutions), по повышению осведомленности (awareness raising) и секретариат.

В 2008 году структура немного изменилась[51]. В помощь Исполнительному директору были добавлены бухгалтерия, служба безопасности, ассистент, веб-мастер (который вместе с отделом по связям с общественностью взаимодействует с департаментом по взаимодействию и поддержке). В структуре департаментов также произошел ряд изменений:

1. в техническом департаменте добавился отдел Security Tools and Architecture и технический отдел, но убрали отдел по технологиям сетевой и информационной безопасности
2. в департаменте по взаимодействию и поддержке отдел по взаимодействию с органами ЕС и стран-членов ЕС переименовали в отдел по координации деятельности между органами ЕС и органами государств-членов ЕС, соответственно, данному отделу добавился ряд других функций.

С приходом нового исполнительного директора в 2009 году, Удо Хелмбрехта, структура ENISA снова изменилась для осуществления поставленных задач более эффективно, и данная структура существует по сегодняшний день[52]. В распоряжении исполнительного директора теперь есть только личный помощник и два департамента:

1. Департамент по административной работе и поддержке, в котором находятся отделы по человеческим ресурсам агентства (human resources section), по финансам, бухгалтерии и снабжения (Finance, Accounting and Procurement Unit) и IT отдел;
2. Второй департамент - Операционный центр (Core Operations Department), в котором находятся отделы по безопасной инфраструктуре и обслуживанию (secure infrastructure and services Unit), по защите информации и данных (information

51 General report 2008 [Electronic resource] / European Network and Information Security Agency. 2009. URL: https://www.enisa.europa.eu/publications/programmes-reports/enisa_gr_2008.pdf (Дата обращения 17.03.16) p. 37

52 см. приложение 5

security and data protection unit), по оперативной безопасности (operational security Unit), по управлению качеством и данными (Quality and Data management unit).

В настоящий момент административный департамент отвечает за то, чтобы работа агентства проводилась в установленных рамках, которые включают в себя финансовый регламент, регламент по персоналу, регламент о внутренней работе органов ENISA и различные механизмы внутреннего контроля.[53] Операционный центр занимается поддержанием высокого уровня профессионализма политических деятелей Европейского союза в области сетевой и информационной безопасности; оказанием помощи государствам-членам и органам европейского союза, а также частному сектору в наращивании потенциала и приведение своей политики в соответствие с правовыми и нормативными требованиями в области сетевой и информационной безопасности; а также укреплением сотрудничества между государственными органами, органами Европейского союза и заинтересованными сторонами в данной области.

Стоит отменить, что изменение структуры упростило ее и уменьшило количество необходимого персонала. Это, во-первых, принесет дополнительную экономию средств для агентства, а значит, данные средства будут вложены в непосредственную деятельность по обеспечению кибербезопасности (согласно последнему отчету, количество человек, работающий в операционном отделе составляет уже 68%[54], что, скорее всего, увеличит эффективность работы); во-вторых, по сравнению с прошлыми видами организации внутренней работы, именно последний вид является наиболее эффективным: теперь операционный департамент разделяет отделы по сферам защиты, а не выделяет отдельно работу с органами власти, работу с организациями и так далее. Можно сказать, что именно сейчас агентство действительно объединяет усилия органов, институтов, агентств Европейского союза и частного сектора для обеспечения безопасного киберпространства и предотвращения киберугроз.

---

53 Work programme 2016 Including multiannual planning [Electronic resource] / European Union Agency for Network and Information Security. 2015. URL: https://www.enisa.europa.eu/publications/programmes-reports/enisa-work-programme-2016 (Дата обращения 17.03.2016) p.49

54 Annual Activity Report 2014 [Electronic resource] / ENISA. 2015. URL: https://www.enisa.europa.eu/publications/programmes-reports/enisa-annual-activity-report-2014 (Дата обращения 17.03.16) p.48

Исполнительному директору по разработке рабочей программы для агентства помогает группа заинтересованных сторон – Permanent Stakeholders' Group (PSG). Данная группа включает в себя представителей индустрии информационно-коммуникационных технологий, провайдеров электронных коммуникационных сетей и сервисов для пользователей, пользовательские группы, академических экспертов в области информационной и сетевой безопасности, а также представителей правоохранительных органов и национальных контролирующих органов.[55] Данная группа помогает поддерживать и развивать взаимоотношения агентства с заинтересованными сторонами в частном секторе, но представители группы заинтересованных сторон не являются сотрудниками Европейского агентства по сетевой и информационной безопасности. Количество представителей в PSG не должно превышать 33 человека, трое из которых являются уполномоченными представителями от Европейского регулирующего органа по электронным коммуникациям, от рабочей группы по защите данных (Article 29 Data Protection Working Party[56]) и от Европола[57], а остальные утверждаются правлением по представлению Исполнительного директора и уполномоченных представителей.[58]

В помощь работе агентству также существует сеть национальных сотрудников по связи (National Liaison Officers network) по одному от каждого государства-члена Европейского союза, Европейской ассоциации Свободной торговли, Европейской комиссии и Совета Европейского союза. Данная сеть не базируется на основе ENISA, но имеет большое значение для агентства, так как помогает поддерживать тесный контакт с государствами-членами ЕС, и усиливает тем самым работу агентства в данных государствах.[59]

---

55 Decision No MB/2014/7 of the Management Board of the European Union Agency for Network and Information Security on the establishment and operation of the Permanent Stakeholders' Group [Electronic resource] / ENISA. 2014. URL: https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/mb-decision-no-mb-2014-7-on-internal-rules-of-operation-of-psg (Дата обращения 17.03.16)

56 Article 29 Working Party [Electronic resource] / European Commission. URL: http://ec.europa.eu/justice/data-protection/article-29/index_en.htm (Дата обращения 17.03.16)

57 Acts adopted under title VI of the EU Treaty council decision establishing the European Police Office (Europol) [Electronic resource] / Official Journal of the European Union. 2009. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:121:0037:0066:en:PDF (Дата обращения 17.03.16)

58 Ibid., Decision of the Management Board…

Ключевым инструментом для для защиты информационных инфраструктур критической значимости является CERT - Computer Emergency Response Teams или Компьютерная программа быстрого реагирования. Данные команды существуют в государстве ЕС и призваны быть основным поставщиком услуг безопасности для государства и граждан, а также заниматься просветительской деятельностью.[60] Однако не все государства обладают такой командой, поэтому миссия ENISA обеспечить их данным органом – в странах Европы и за ее пределами. Кроме того, ENISA находится в постоянном взаимодействии со всеми CERTs. В будущие планы агентства входит дальше поддерживать создание подобных органов, создавать отчеты о передовом опыте в области кибер инцидентов с помощью CERTs, советовать государствам-членам ЕС в улучшении IT инфраструктуры, а также тестировать CERTs.

Несмотря на то, что нынешняя структура агентства является наилучшим вариантом из того, что было, она все равно несколько запутана и нуждается в дальнейшем улучшении. Агентству следовало бы разместить на сайте отдельный раздел, в котором были бы отражены все внутренние элементы и горизонтальные связи между ними и то, как они взаимодействуют со вспомогательными командами. Четкая иерархия поможет ENISA наиболее эффективно выполнять возложенные на него задачи.

2.2 ЭКОНОМИЧЕСКИЕ РЕСУРСЫ АГЕНТСТВА ПО СЕТЕВОЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

При построении бюджета, агентство руководствуется рядом принципов, прописанных в регламенте ENISA по финансовым вопросам[61]:

---

59 NLO Network [Electronic resource] / ENISA. URL: https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office (Дата обращения 17.03.2016)

60 CERT [Electronic resource] / ENISA. URL: https://www.enisa.europa.eu/activities/cert (Дата обращения 4.04.2016)

61 DECISION No MB/2014/1 WP Of the Management Board of the European Union Agency for Network and Information Security (ENISA) The financial regulation applicable to the European Union Agency for Network and Information Security in conformity with the Commission Delegated Regulation (EU) No 1271/2013 of 30 September 2013 on the framework financial regulation for the bodies referred to in Article 208 of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council [Electronic resource] / ENISA. 2014. URL: https://www.enisa.europa.eu/about-enisa/accounting-finance/files/enisa-financial-regulation-1 (Дата обраения 21.03.16)

1. Первый принцип – принцип единства и точности бюджета (Principles of unity and of budget accuracy) означает, что каждый год все доходы и расходы агентства должны быть включены в единый документ – бюджет агентства. Бюджет ENISA включает в себя: добровольные пожертвования государств-членов Евросоюза в денежной или натуральной форме; вклады от самого Европейского союза; взносы от третьих стран, участвующих в работе агентства; расходы агентства, включая административные. Агентство также может получить гранты от Европейского союза при условии, что данные гранты будут включены в годовую рабочую программу ENISA. Согласно регламенту, агентство не может получать дохода, если данные доходы не были включены в рабочий бюджет; ENISA также не может превышать запланированные в бюджете траты;
2. Второй принцип – принцип ежегодности (Principle of annuality) предполагает, что бюджет должен формироваться на один финансовый год, который, согласно регламенту, начинается 1 января и заканчивается 31 декабря. Согласно данному принципу, каждый финансовый год агентство делает отчет о выручке ENISA, данная выручка должна покрывать выделенные агентству ассигнования, которые должны тратиться только на расходы ENISA. Ассигнования выделяются агентству сразу же после одобрения агентством 1 января своего нового годового бюджета;
3. Третий принцип – принцип баланса (Principle of equilibrium) подразумевает, что доходы и расходы агентства должны находиться в равновесии. Если бюджет на конец года положителен, то данный доход передается Комиссии ЕС, которая часть из этого дохода определяет агентству на следующий финансовый год для расходов. Если же бюджет на конец года отрицателен, то данные средства переводятся либо как долг на будущий финансовый год для агентства, либо в качестве противовеса для положительного бюджета за прошлый финансовый год;
4. Четвертый принцип – принцип единицы счета (Principle of unit of account) заключается в том, что все расходы и доходы должны вестись в денежной единице евро;
5. Пятый принцип – принцип универсальности (Principle of universality) – все доходы должны использоваться для конкретной статьи расходов. Существуют внешние доходы (взносы стран-членов Европейского союза и третьих стран, доходы от грантов и т.д) и внутренние (выручка от третьих сторон за предоставленные им услуги, доходы от продажи оборудования, научно-технических материалов, страховые платежи и т.д.);

6. Пятый принцип – принцип детализации (Principle of specification) – ассигнования должны определяться на конкретные цели под определенным заглавием, каждое заглавие должно разделяться на статьи. Исполнительный директор может перебрасывать ассигнования на другие отделения не более чем на 10% от всего объема ассигнований, а между статьями расходов в одном отделении количество переброcов неограниченно;
7. Шестой принцип – принцип эффективного финансового управления (Principle of sound financial management) предполагает, что предоставляемые агентству ассигнования должны использоваться в соответствии с принципами экономии, эффективности и результативности, а значит, что агентство должно выискивать ресурсы наиболее выгодные по качеству и цене, стараться добиваться отличных результатов от данных ресурсов, а также нужно постоянно с помощью данных ресурсов достигать поставленных агентством целей. Информация о достижения в каждом конкретном виде деятельности должна предоставляться ежегодно правлению. Агентство также должно проводить ex ante и ex post оценку деятельности в соответствии с указаниями Комиссии для того, чтобы улучшить процесс принятия решений, после чего Исполнительный директор подготавливает план действий по финансовым тратам;
8. И последний принцип – принцип прозрачности (Principle of transparency) предполагает опубликование всех принятых бюджетов и внесенные к ним изменения в официальном журнале Европейского союза (не позднее 3 месяцев), а также на сайте агентства (не позднее 4-5 недель).

В общей сложности, агентство создает два вида рабочих программ – годовые программы и многолетние[62]. Многолетние программы включают в себя, согласно регламенту, общие цели агентства на будущее, ожидаемые результаты деятельности, программу по распределению ресурсов. Ежегодная программа включает в себя детализированные цели и ожидаемые результаты, а также содержит информацию о

62 DECISION No MB/2014/1WP Of the Management Board of the European Union Agency for Network and Information Security (ENISA) on the financial regulation applicable to the European Union Agency for Network and Information Security in conformity with the Commission Delegated Regulation (EU) No 1271/2013 of 30 September 2013 on the framework financial regulation for the bodies referred to in Article 208 of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council [Electronic resource] / ENISA. 2014. URL: https://www.enisa.europa.eu/about-enisa/accounting-finance/files/enisa-financial-regulation-1 (Дата обращения 21.03.16) p. 23

будущей деятельности и предполагаемых затрат (финансовых и людских) на данные действия. Данная программа согласовывается с многолетним планом работы, в ней также должны быть отражены все цели и задачи, которые были изменены или добавлены.

Бюджет агентства должен состоять из двух основных частей:

1. Первая часть – отчет о выручке, в котором прописывается предполагаемая прибыль агентства за финансовый год, доход за предшествующий финансовый год и пометки.

2. Вторая часть – отчет о расходах, разделенный на три общих статьи, каждая из которых делиться на конкретные статьи расходов.

Кроме того, агентство после окончания финансового года выпускает бухгалтерский отчет о работе, в котором также отражено количество полученных за год доходов (которое может отличаться от цифры, написаной в бюджете) и количество расходов, а также отчет об исполнении бюджета. После этих данных вычисляется, является ли бюджет за данный финансовый год положительным или отрицательным. Для определения итогового баланса используется не просто вычет расходов из доходов, но также информация о том, были ли использованы ассигнования, которые перечислили с прошлого финансового года; информацию о курсе валюты (потеряли ли на этом, и если да, то сколько) и так далее. Кроме того, по итогам финансового года выпускается отчет от европейского суда аудиторов о том, какие задачи выполнило агентство за прошлый финансовый год.

Исходя из того, что в распоряжении на данный момент касательно 2016 года есть только план работы (годовой и многолетний), касательно 2015 года есть план работы, бюджет, а касательно 2014 года есть план работы, бюджет и все отчеты о работе за 2014 финансовый год в свободном доступе, то в данной работе эффективность деятельности агентства будет рассматриваться, начиная с 2014 года.

В рабочей программе за 2014 год стоит три основных рабочих направления: помощь в построение европейского политики (support EU policy building), помощь в повышении возможностей (support capacity building), поддержка сотрудничества (support cooperation).

Для помощи в построении политики Европейского союза в области кибербезопасности, агентство выделило для себя три основных рабочих пакета –

деятельность по выявлению угроз, способствование политическим инициативам, поддержка в научных исследованиях.

Основной целью комплекса мероприятий по выявлению угроз, рисков и вызовов являлось сбор и обработка информации для развития ежегодного отчета ENISA о ситуации с угрозами – в данном документе рассматриваются появление новых видов угроз, их описания, а также тренды по падению или усилению уже существующих угроз. Для данных задач прописана необходимая стоимость в 100 000 евро[63].

Целью же способствования политическим инициативам Европейского союза являлись обеспечение ввода новых политических инициатив, помощь Европейской комиссии и государствам-членам в эффективном осуществлении данной политики, а также в получении опыта для избегания проблем в будущем. Стоимость данных задач ENISA оценила в 140 000 евро.[64]

И последним комплексом мер являлись поддержка ЕС в образовании, научных исследованиях и стандартизации, цель которого было развитие сотрудничества с координационной группой по кибербезопасности (Cyber Security Coordination Group, CSCG). На данную задачу запрошено 40 000 евро.[65]

Согласно годовому отчету о работе[66], основные задачи по данному направлению выполнены на 100%:

1. ENISA хотела добиться того, чтобы как минимум 10 международных информационных изданий, посвященных безопасности, ссылались на рапорт ENISA об угрозах, который называется «Threat Landscape» - в итоге на отчет об угрозах за 2014 год сослались более чем 20 различных организаций;

63 Work Programme 2014 [Electronic resource] / ENISA. 2013. URL: https://www.enisa.europa.eu/publications/programmes-reports/work-programme-2014 (Дата обращения 23.03.16) p.19

64 Ibid., p24

65 Work Programme 2014 [Electronic resource] / ENISA. 2013. URL: https://www.enisa.europa.eu/publications/programmes-reports/work-programme-2014 (Дата обращения 23.03.16) p. 26

66 Annual Activity Report 2014. [Electronic resource] / ENISA. Publications Office of the European Union. 2014 URL: https://www.enisa.europa.eu/publications/programmes-reports/enisa-annual-activity-report-2014 (Дата обращения 28.03.2016) p. 10

2. При этом достигнута и вторая задача – ENISA хотела, чтобы ссылались заинтересованные стороны из двух разных секторов, в результате вышло три сектора – интернет инфраструктура, «умный дом» и медиа;
3. Последняя задача включала в себя необходимость вовлечения отчета о новых рисках и угрозах как минимум в пять проектов научно-исследовательских и опытно-конструкторских работ. В результате же большинство угроз, выявленных ENISA, были использованы в проектах «Горизонт 2020» и так далее

Второстепенные задачи по подготовке отчетов о новых угрозах, созданию гайдов, действий по стандартизации и т.д. также выполнены, согласно отчету.

Следующее направление – поддержка в построении возможностей – нацелено на поддержку ключевых заинтересованных сторон в развитии операционных и политических возможностей для решения различных проблем кибербезопасности. Данная цель должна быть достигнута путем сбора, обработки и распространения полезных знаний для государственного и частного секторов.[67] Основные мероприятия разделяются по объектам деятельности: поддержка государств-членов Европейского союза (Support Member States' Capacity Building), поддержка частного сектора (Support Private Sector Capacity Building), повышение уровня подготовки граждан Европейского союза (Raising the level of preparedness of EU citizens).

Мероприятия для государств направлены на развитие методов профилактики, обнаружения, анализа и реагирования по вопросам кибербезопасности в институтах, как государств-членов ЕС, так и в общеевропейских институтах и органах. Для данной цели запрошено 290 000 евро.[68]

Целью же мероприятий для частного сектора является повышение возможностей путем кооперации усилий с государственным сектором через облачные вычесления (Cloud Computing), умные сети электроснабжения (smart grids) и через Electronic Communication Network (електронная система осуществления сделок купли-продажи на бирже). Для данных мероприятий определена необходимая сумма в 185 000 евро.[69]

67 Ibid., work programme… (Дата обращения 28.03.2016) p. 27

68 Work Programme 2014 [Electronic resource] / ENISA. 2013. URL: https://www.enisa.europa.eu/publications/programmes-reports/work-programme-2014 (Дата обращения 28.03.16) p. 32

69 Ibid, p. 36

И последний комплекс мероприятий для данного направления – повышение уровня подготовки граждан Европейского союза – нацелен на поддержку просветительской и учебной деятельности в государствах– членах ЕС для безопасного использования информационно-коммуникационных технологий, а также на помощь в организации месяца кибербезопасности. Для данных мероприятий поставлена необходимая сумма в 20 000 евро.[70]

Согласно отчету о работе за 2014 год, основным достижением по данному направлению является проведение очередного месяца кибербезопасности в Европе (European Cyber Security Month), который проводится ежегодно, начиная с 2011 года. Основными направлениями работы являлись различные тренинги для студентов, граждан Евросоюза, технических экспертов, государственных и частных организаций.[71] Кроме того показатели эффективности, которые были установлены ENISA в рабочей программе, по данному направлению также перевыполнены – как основные, так и второстепенные.

И последним рабочим направлением является поддержка сотрудничества, которое должно гарантировать усиление сетевой и информационной безопасности внутри Европейского союза для того, чтобы Европа была важным игроком на международной арене в этой сфере.[72] Кооперация должна обеспечиваться путем обмена знаниями в области информационной и сетевой безопасности между государствами-членами ЕС, европейскими институтами и другими заинтересованными сторонами (третьими странами, частным сектором). Частными целями также являлись организация мероприятия Кибер Европа 2014 года, развитие дальнейшего сотрудничества ENISA с Центром интерпола по кибербезопасности и т.д. Основные мероприятия включают в себя: сотрудничество в кризисных учениях, а именно подготовка мероприятия Европейские кибер учения 2014 (на данную работу запрошено 201 500 евро); внедрение законодательства в Европейский союз, а именно, во-первых, продолжение работы с подготовкой отчета о киберинцедентах, а во-вторых, разработка директивы об

70 Ibid, p. 38

71 What's ECSM [Electronic resource] / ENISA. URL: https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign (Дата обращения 29.03.2016)

72 Work Programme 2014 [Electronic resource] / ENISA. 2013. URL: https://www.enisa.europa.eu/publications/programmes-reports/work-programme-2014 (Дата обращения 28.03.16) p. 39

электронных трастовых операциях и электронной идентификации (которая была принята в 2014 году)[73], на что запрошено 130 000 евро[74]; регулярное взаимодействие между сообществами по информационной и сетевой безопасности, в частности между CERT и правоохранительными органами (на данный комплекс мероприятий запрошено 127 500 евро)[75].

Данное направление также не осталось в стороне: множество участников было привлечено для участия в мероприятии «Кибер Европа 2014», все участники выразили удовлетворенность прошедшими учениями и рекомендациями ENISA. Необходимое количество участников было привлечено и в работу на 9 встрече ENISA CERT, а также многие поддержали обмен информацией между компьютерными командами быстрого реагирования различных государств и организаций (в частности, привлекли к обмену опытом Siemens и Panasonic).

В рабочей программе также отражаются предполагаемые траты на работу секретариата правления, исполнительного комитета и группы заинтересованных сторон (260 000 евро), на корпоративную коммуникацию (50 000 евро), на деятельность по распространению знаний (40 000 евро). И отдельным пунктом указываются траты на внутреннюю работу и деятельность административного департамента: например, закупка каких-то книжных материалов, подготовка бюджета, работа HR отдела, работа IT отдела и т.д. Больше всего выделяется на HR – 5 947 226 евро. Всего на работу департамента выделяется 7 002 354 евро.

Всего на деятельность ENISA в 2014 году в рабочей программе было определено 9 086 354 евро[76], данная цифра и была определена в бюджет на 2014 финансовый год. Позже, в дополнениях к бюджету, были сокращены расходы на персонал, на активность по обеспечению сотрудничества заинтересованных сторон в области сетевой и информационной безопасности, но увеличены на работу в области технологий сетевой и

---

73 Regulation (EU) No 910/of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [Electronic resource] / Official Journal of the European Union. 2014. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG (Дата обращения 03.2016)

74 Ibid., work programme… p. 45

75 Ibid, p. 47

76 см. Приложение 6

информационной безопасности, обслуживание существующих систем ИКТ агентства, на переход к новым системам и на обслуживание телекоммуникации, хостинга и т.д. Таким образом, бюджет был увеличен до 9 708 296, 66 евро.[77] По результатам финансового года, бюджет оказался положительным – во-первых, количество расходов было меньше, чем запланировано в бюджете, во-вторых, доходы выше расходов (хотя и меньше, чем было запланировано в бюджете).

Исходя из того, что бюджет на данный финансовый год оказался положительным, что все задачи ENISA на 2014 год были выполнены можно сделать вывод о том, что в 2014 году ENISA показала себя с отличной стороны. Об этом говорит еще и то, что в бюджете 2015 года уже выделено больше средств, в том числе увеличены траты на деятельность агентства за счет сокращения средств на персонал и базовые расходы (рента, оплата коммунальных счетов и т.д.)[78]. Кроме того, в рабочей программе 2015 года появились 4 стратегические цели (которые входят в многолетний план работы до 2017 года) вместо направлений работы – развивать и поддерживать высокий уровень профессионализма европейских акторов, учитывая эволюцию сетевой и информационной безопасности; помогать в укреплении потенциала на территории всего Европейского союза; оказывать поддержку государствам-членам ЕС и Комиссии в разработке и реализации стратегий необходимых для соблюдения законодательных и нормативных требований по сетевой и информационной безопасности; расширять сотрудничество между государствами-членами ЕС и обществами, связанными с сетевой и информационной безопасностью.[79] А в рабочей программе 2016 года снова планируется увеличение расходов на деятельность практически на 1 000 000 евро.[80] Причем упор делается больше на укрепление потенциала

77 Amending Statement of Estimates no 02/2014 (Amending Budget no 02/2014) [Electronic resource] / the European Union Agency for Network and Information Security. 2014. URL: https://www.enisa.europa.eu/about-enisa/accounting-finance/files/annual-budgets/enisa-amending-budget-2-2014 ((Дата обращения 29.03.2016) p. 4

78 Amending Statement of Estimates no 01/2015 (Amending Budget 2015) [Electronic resource] / the European Union Agency for Network and Information Security. 2015. URL: https://www.enisa.europa.eu/about-enisa/accounting-finance/files/annual-budgets/amending-budget-1-2015-final (Дата обращения 29.03.2016) p. 4

79 Work Programme 2015 Including Multi-Annual Planning [Electronic resource] / the European Union Agency for Network and Information Security. 2014 URL: https://www.enisa.europa.eu/publications/programmes-reports/enisa-work-programme-2015 (Дата обращения 29.03.2016) p. 20

80 Work programme 2016 Including multiannual planning [Electronic resource] / European Union Agency for Network and Information Security. 2015 URL: https://www.enisa.europa.eu/publications/programmes-reports/enisa-work-programme-2016 (Дата обращения 23.03.2016) p. 56

государственного и частного секторов и на разработку стратегий по соответствию требованиям сетевой и информационной безопасности, что говорит нам о работе в текущем году, в основном, над законодательством в данной сфере, например, над стратегией кибербезопасности, в разработке которой ENISA оказало существенную помощь в прошлом.

ГЛАВА 3. ДЕЯТЕЛЬНОСТЬ ENISA И ПЕРСПЕКТИВЫ РАЗВИТИЯ АГЕНТСТВА.

3.1 СОТРУДНИЧЕСТВО С ENISA В РАЗРАБОТКЕ ОБЩЕЕВРОПЕЙСКОЙ И НАЦИОНАЛЬНЫХ ЕВРОПЕЙСКИХ СТРАТЕГИЙ КИБЕРБЕЗОПАСНОСТИ.

7 февраля 2013 года Европейской Комиссией и Верховным представителем Союза по иностранным делам и политике безопасности было объявлено об общеевропейской стратегии кибербезопасности и о предложениях по отношению к Директиве «О мерах по обеспечению высокого общего уровня кибербезопасности в странах Европейского союза». Исполнительный директор ENISA Удо Хельбрехт отметил, что Комиссия достигла огромного успеха, поскольку благодаря данной стратегии у Европейского союза теперь есть направление для деятельности, которым будут также руководствоваться внутри государств-членов для построения безопасного киберпространства внутри своих стран.[81] Само агентство оказывало поддержку в разработке общеевропейской стратегии, а в 2015 году Европейский совет издал документ об обновлении стратегии кибербезопасности, в котором говорилось, что помимо прочих агентств, ENISA, через создание рабочих групп, также будет вовлечено в разработку новой стратегии.[82] Кроме того, агентство активно помогало с разработкой национальных стратегий кибербезопасности (НСК) тем, что анализировала существующие национальные стратегии, предлагала планы по разработке и реализации НСК, осведомляла об успешных проектах по реализации стратегий для того, чтобы государства-члены ЕС могли оценить и исправить свои стратегии. Например, в декабре 2012 году ENISA издала практическое руководство по развитию и исполнению национальной стратегии кибербезопасности, которое представляет собой набор действий, выполнение которых приведет к реализации успешной национальной кибер стратегии.[83]

---

81 New EU Cybersecurity strategy & Directive announced [Electronic resource] / ENISA. 2013. URL: https://www.enisa.europa.eu/media/news-items/new-eu-cybersecurity-strategy-directive-announced (Дата обращения 30.03.2016)

82 Draft Council Conclusions on the Renewed European Union Internal Security Strategy 2015-2020 [Electronic resource] / Council of the European Union. 2015. URL: http://statewatch.org/news/2015/jun/eu-council-iss-draft-conclusions-9416-15.pdf (Дата обращения 6.04.2016) p. 10

83 National Cyber Security Strategies. Practical Guide on Development and Execution [Electronic resource] / European Network and Information Security Agency. 2012. URL: https://www.enisa.europa.eu/activities/Resilience-

В общеевропейской стратегии[84] дается 5 ключевых целей для решения проблем по кибербезопасности:

1. Обеспечение устойчивости киберпространства Европейского союза;
2. Сокращение количества киберпреступлений;
3. Развитие политики кибероборонына основе Общей политики безопасности и обороны Европейского союза;
4. Развитие производственно-технологических ресурсов для обеспечения кибербезопаности;
5. Создание согласованной всеми членами Евросоюза международной политики по кибербезопасности с иностранными парнерами для повышения кооперации в данной области с третьими странами.

Для первой цели[85] отмечается необходимость кооперирования усилий частного сектора с государственным, для чего в прошлом была создана политика «Сетевой и информационной безопаности» (Network and Information Security, NIS), а так же была организовано ENISA. Кроме того, предлагаются такие шаги, как создание национальных стратегий кибербезопасности и органа, ответственного за политику в данной сфере в каждом государстве-члене; создание механизма обмена данными между этими органами.

Для второй цели[86] необходимо принять определенное законодательство в области кибербезопасности, которое помогло бы кооперировать силы стран — членов Европейского союза в борьбе с киберпреступниками. Одним из первых шагов, которые отмечает стратегия, должно стать подписание всеми государствами ЕС Будапештской конвенции о киберпреступности (принятой в 2001)[87], в которой содержится перечень преступлений в киберпространстве. Данные преступления должны быть прописаны в

---

and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide (Дата обращения 30.03.2016)

84 Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [Electronic resource] / Brussels. 2013. URL: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf (Дата обращения 30.03.2016) p. 4-5

85 Ibid., p. 5

86 Ibid., p. 9-10

87 CONVENTION ON CYBERCRIME [Electronic resource] / Budapest. 2001. URL: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (Дата обращения 30.03.2016)

уголовном законодательстве стран, подписавших конвенцию, и, соответственно, приносить с собой вполне реальный тюремный срок в случае нарушения.

Третья цель[88] предполагает, согласно стратегии, содействие развитию кибероборонны Европейского союза с помощью различных средств и технологий: например, доктрин, органов, обучения специализированного персонала, проведения тренингов, развития технологий и инфраструктуры. Кроме того, отмечается необходимость тестного сотрудничества в данной области на международной арене, в особенности с НАТО.

Касательно последних двух целей[89], стратегия отмечает, что Европейскому союзу требуется создать свой собственный рынок информационно-коммуникационных безопасный технологий для того, чтобы избежать зависимости от поставок, а также развивать международное сотрудничество по кибербезопасности, в особенности с США в рамках рабочей группы по кибербезопасности и киберпреступлениям.

Таким образом, общеевропейская стратегия кибербезопасности не носит характер практического руководства с конкретными шагами по его реализации; это всего лишь общее направление работы, основываясь на котором каждое государство, при помощи агентства по сетевой и информационной безопасности, создает собственную стратегию по кибербезопасности. К основному минусу общеевропейской стратегии можно отнести отсутсвие четкого понятийного аппарата: если бы в Европе существовало единое понятие о терминах «киберпространство», «кибербезопасность» и так далее, то на национальных уровнях реализация политики в этой новой сфере проходила бы намного быстрее. На данный момент выходит так, что в каждой национальной стратегии есть свое определение: например, в финской стратегии[90] дается определение слова «кибер» как «совокупность электронной переработки данных, информационных технологий, электронной коммуникации, информационных и компьютерных систем», а в испанской стратегии[91] уже

88 Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [Electronic resource] / Brussels. 2013. URL: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf (Дата обращения 30.03.2016) p. 11

89 Ibid., p. 12-15

90 Finland´s Cyber security Strategy [Electronic resource] / Finland. : Forssa print, 2013. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/FinlandsCyberSecurityStrategy.pdf (Дата обращения 31.03.2016) p. 13

91 NATIONAL CYBER SECURITY STRATEGY [Electronic resource] / Spain. 2013. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-

несколько другое определение киберпространства: «глобальная предметная область, включающая в себя информационные технологии, информационные и телекоммуникационные системы (включая Интернет — сети), которая не имеет границ, вовлекая тем самым своих пользователей в глобализацию».

А вот национальные стратегии являются конкретными рекомендациями, которым необходимо обновляться в связи с новой информацией, появлением новых угроз и способов борьбы с ними. В этом государствам-членам ЕС активно помогает ENISA. С появления первых европейский национальных стратегий (2011 год, Великобритания, Румыния, Германия, Чешская республика, Литва) прошло уже практически 5 лет – с этого времени ENISA активно вело работу по анализу существующей ситуации в киберсфере, выпустило множество практических рекомендаций, провело несколько общеевропейских мероприятий по кибербезопасности. На данный момент уже 23 государства – члена Европейского союза обладают национальными стратегиями по кибербезопасности, большинство из которых начали появляться после выпуска руководства ENISA по внедрению НСК в 2012 году – «Национальные стратегии по кибербезопасности: руководство по осуществлению» – в котором собрали практические шаги по реализации целостной национальной стратегии кибербезопасности, а также описали показатели эффективности, на которые следует ориентироваться; кроме того, в 2012 году ENISA выпустило статью «Национальные стратегии кибербезопасности»[92], которая включала в себя анализ уже существующих европейских и международных стратегий кибербезопасности, а также серию рекомендаций по внедрению и усовершенствованию НСК на краткосрочный и долгосрочный периоды.

В 2014 году, спустя 2 года после последнего руководства, ENISA решило выпустить новый доклад по усовершенствованию национальных стратегий кибербезопасности, который называется «Механизм оценки национальных стратегий кибербезопасности»[93] и

ncsss/NCSS_ESen.pdf (Дата обращения 31.03.2016) p. 11

92 National Cyber Security Strategies [Electronic resource] / European Union Agency for Network and Information Security. 2012. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper (Дата обращения 31.03.2016)

93 An evaluation Framework for National Cyber Security Strategies [Electronic resource] / European Union Agency for Network and Information Security. 2014. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1 (Дата обращения 31.03.2016)

состоит из набора индикаторов для оценки эффективности НСК. В частности, так предлагается использование логической модели, которая показывает взаимосвязи между входными данными, процессами, промежуточными и конечными результатами в развитии стратегии кибербезопасности. В данной модели выделены 5 направлений[94], который должны учитываться:

1. развитие политики и возможностей для кибер защиты (участие в инициативах ЕС в данной области, построение возможностей, техническое развитие);
2. достижение кибер устойчивости: развитие сотрудничества и возможностей между государственным и частным сектором (представлять анализы кибер рисков на национальном уровне, участвовать в национальных и международных кибер учениях, уделять время обучению, укрепление потенциала общества);
3. снижение киберпреступлений (повышение возможностей борьбы с трансграничными киберпреступлениями; снижение барьеров для расследований; использовать современные инструменты борьбы с киберпреступлениями);
4. развитие промышленных и технологических ресурсов для кибербезопасности; защита инфраструктуры объектов критической значимости (создание планов по управлению рисками и планов по обеспечению устойчивости бизнеса;
5. создание надежных механизмов обмена информацией между государственным и частным секторами).

По этим же направлениям в данном руководстве отмечены ключевые показатели эффективности, которые сделают анализ национальной стратегии более сфокусированным и результативным. По каждому направлению выделено от 5 до 9 показателей эффективности, напротив каждого отмечены доказательство того, что данный показатель выполнен. Рассматривать все показатели нет необходимости, но как пример можно привести один – для второго направления (достижение устойчивости) показателем эффективности является создание CERT и/или национального агентства по безопасности, а доказательством выполнения данного показателя является наличие мандата у такого институционального органа.

Данный документ от агентства должен помочь государствам – членам Европейского союза провести глобальный анализ своей существующей стратегии и создать для себя план действий по дальнейшему развитию НСК. Однако агентство по сетевой и информационной безопасности могло бы принести еще больше пользы, учитывая наличие

94 Ibid., p. 28-29

в своем распоряжении экспертов со всего Европейского союза. ENISA могло бы обеспечить постоянный анализ каждой из существующих стратегий кибербезопасности в государствах-членах ЕС (то есть, государство диллегировало бы данную задачу агентству), создавало бы отчет о данной стратегии и публиковало бы его для того, чтобы другие государства также могли на него ориентироваться – поскольку в интересах всего Европейского союза обеспечить самый высокий уровень кибербезопасности в каждом члене ЕС, а создать «идеальную» стратегию, которая была бы актуальна сразу для всех, невозможно, потому что у каждого государства свои ресурсы, свои проблемы и задачи. Кроме того, агентство может быть главным центром по разработке предложений об изменении общеевропейской стратегии, чтобы снять эту задачу с других органов Европейского союза – в таком случае, ENISA могло бы заниматься разработкой общих механизмов для ЕС в сфере кибербезопасности, которые отражались бы в новых редакциях европейской стратегии. Данная задача может быть осуществлена ENISA, поскольку в состав правления входят предстовители от каждого государства (которые смогут продвигать предложения от своих стран, а значит разрабатываемые механизмы будут подходящими для каждого государства), кроме того, ENISA обладает большой группой экспертов из различных сфер и стран, а следовательно, разрабатываемые механизмы будут не поверхностными, а охватывающими и государственные и частные интересы.

3.2 УСПЕШНЫЕ ДЕЙСТВУЮЩИЕ ЕВРОПЕЙСКИЕ ПРОЕКТЫ АГЕНТСТВА ПО СЕТЕВОЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Напомним, что основополагающей целью агентства является повышение кибер культуры среди государственного, частного секторов и граждан Европейского союза в целом. Для этого за практически 12 лет своей работы агентство организовало несколько постоянно действующих проектов по кибер учениям, а также часто выпускает полезные статьи на тему киберсферы – часть из которой является переодическими изданиями, а часть разовыми. Кроме того, агентство активно участвует в таргетированной помощи государствам-членам Европейского союза, например, в разработке и внедрении национальных стратегий, о чем писалось выше. Для оценки эффективности работы в данной исследовании использованы материалы об успешных фактических постоянно действующих проектах (Европейский месяц кибербезопасности, Кибер Европа, кибер учения) и об успешных публикующихся на регулярной основе материалах (Обзор угроз ENISA, Ежегодный отчет о кибер инцидентах).

В проведении кибер учений ENISA не работает в одиночку: ему оказывают содействие ряд автономных агентств, специально созданных для разрешения различного рода задач.[95] К ним относятся:

1. агентства сообщества (например, агентство безопасного морского сообщения - EMSA, агенство авиационной безопасности - EASA и так далее);
2. агентства по внешней политике и политике безопасности (например, оборонное агентство – EDA);
3. полицейские и судебные агентства (например, полицеское ведомство Europol);
4. временные исполнительные агентства (например, агентство по образованию, аудиовизуальным средствам и культуре – EACEA);
5. Центр по борьбе с киберпреступностью (European cyber security center – ECCC).

В 2012 году ENISA опубликовало аналитический отчет с фактическими сравнениями о проведенных киберучениях в период с 2002 по 2012 года, что включает в себя 85 кибер

95 Петренко А.А, Петренко С. А. Киберучения: методические рекомендации ENISA // Вопросы кибербезопасности – 2015. №3(11) – С.5

учений. Согласно данному отчету, более 84 стран приняло участие в международных кибер учениях и более 22 европейских государств во внутренних учениях.[96]

По данному отчету, типовыми целями киберучений являются[97]:

1. повышение осведомленности о киберсфере;
2. оценка способности государственных и коммерческих структур к реагированию на кибер инциденты;
3. построение эффективного взаимодействия между государственным и частным секторами;
4. повышение доверия среди государств, повышение сотрудничества между государствами и другие.

Только одно киберучение было организовано коммерческой структурой, а не государственной, что говорит о том, что частный сектор вовлечен недостаточно сильно в повышение осведомленности о киберсфере.[98]

Помимо проводимых государствами кибер учений, ENISA ежегодно проводит Европейский месяц кибербезопасности. Данный проект проводится с целью повышения кибер культуры среди граждан Европейского союза, изменения их восприятия о кибер угрозах посредством обмена знаниями и передовым опытом. В 2012 году вышел первый пилотный проект, который был поддержан европейскими государствами и Комиссией и превратился в ежегодный проект. По окончанию проекта ENISA выпускает различные рекомендации и советы по сетевой и информационной безопасности. В 2014, например, году рекомендации давались для преподавателей в области киберсферы, сотрудников, для программных компаний и пользователей по поводу безопасного программного обеспечения, для технических экспертов, для пользователей облачных хранилищ, а также учения по поводу повышения осведомленности пользователей о своих правах.[99] А в 2015

96 On National and International Cyber Security Exercises: Survey, Analysis and Recommendations [Electronic resource] / European Network and Information Security Agency (ENISA). 2012. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-exercises/exercise-survey2012 (Дата обращения 4.04.2016)

97 Ibid., p. 11

98 Ibid., p. 8

99 ECSM - Recommendations for ALL – EN [Electronic resource] / ENISA. 2014. URL: https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign/2014/ecsm-recommendations-for-all-en (Дата обращения 4.04.2016)

году ENISA провела, кроме прочего, анализ эффективности учений и посредством опроса выяснило, что граждане Европейского союза часто пользуются рекомендациями месяца кибербезопасности, и проводимые учения соответсвуют поставленным задачам.[100]

Кроме месяца кибербезопасности, ENISA, начиная с 2010 года, раз в два года проводит мероприятие «Кибер Европа», которое посвящено повышению доверия к системам управления объектами критической важности. Основными целями последнего мероприятия (в 2014 году) были тестирование возможностей IT систем государств и коммерческих организаций реагировать на международные кибератаки, тестирование систем кооперации Европейского союза, построить и протестировать возможности взаимодействия государственного сектора с частным и частного с частным, а также проанализировать текущее положение дел - есть ли эскалация угроз кибербезопасности.[101] Данный проект зарекомендовал себя с эффективной стороны, потому уже идет планирование «Кибер Европы 2016».

Кроме вышеназванных мероприятий, ENISA осуществляет информационную поддержку путем выпуска различных обзоров и отчетов. Одним из таких отчетов является ежегодный обзор ENISA о киберугрозах (ENISA Threat Landscape - ETL) – последний датируется 2015 годом. Данный доклад обеспечивает информацией о динамике киберугроз примерно за 12 месяцев. На ETL ориентируются государства-члены Европейского союза при построении и улучшении своей национальной стратегии по киберугрозам и различные частные организации. Например, согласно ежегодному отчету о работе ENISA за 2014 год[102], на ETL за 2014 год ссылались более 20 различных организаций, связанных с

---

100 The European Cyber Security Month 2015: Deployment report [Electronic resource] / European Union Agency for Network and Information Security (ENISA). 2015. URL: https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign/2015 (Дата обращения 4.04.2016) p. 15

101 Cyber Europe 2014 – Questions and Answers [Electronic resource] / ENISA. 2014. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2014/cyber-europe-2014-information/briefing-pack/cyber-europe-2014-2013-questions-and-answers (Дата обращения 4.04.2016)

102 Annual Activity Report 2014. [Electronic resource] / ENISA. Publications Office of the European Union. 2014. URL: https://www.enisa.europa.eu/publications/programmes-reports/enisa-annual-activity-report-2014 (Дата обращения 28.03.2016) p. 10

киберсферой, что говорит нам о высокой степени доверия к аналитическим докладам агентства и его деятельности в целом.

Помимо такого обзора киберугроз, ENISA выпускает также ежегодный отчет о кибер инцидентах – Annual Incident Reports.[103] Данный доклад позволяет просмотреть какие инциденты вызвали сбои в системах Европейского союза, что позволяет продумать механизм защиты от подобных угроз в будущем. Например, согласно отчету за 2014 год, основной объем инцидентов был связан со смартфонами и, в большинстве случаев, с техническими ошибками. Данный отчет используется ENISA при построении рабочей программы на будущий год – одной из задач, как правило, является анализирование произошедших инцидентов и выпуск материалов с рекомендациями по борьбе с ними. Такая задача была в рабочих программах и на 2014 год, и на 2015. В 2016 такой задачи не стоит, поскольку больше внимания уделяется улучшению национальных стратегий государств-членов Европейского союза.

Кроме данных постоянных отчетов, ENISA выпускает множество докладов, рекомендаций, новостей по киберсфере. Основные разделы публикаций – CERT, защита объектов критической важности, сопротевляемость, конфеденциальность, CERT новости, оценка угроз, безопасность облачных вычисленний, осведомление о сетевой и информационной безопасности, кибербезопасность, кибератаки и раздел eID. Проанализировав выпуски по годам, можно отследить тендецию увелечения интереса к той или иной тематике – например, в 2014 году большинство публикаций было посвящено теме кибербезопасность, а связанно это с выпуском рекомендаций по улучшению национальных стратегий кибербезопасности. В 2016 году пока что больше внимания уделяется защите критически важных объектов, что связано с основными задачами на текущий год – развитие национальных стратегий, совершенствование знаний об объектах критической важности и так далее. На 2015 год подобных сложных задач еще не стояло, из чего следует, что уровень доверия к агентству возрос, ему доверяют воплощать все более сложные проекты.

---

103 Annual Incident Reports 2014: Analysis of Article 13a annual incident reports [Electronic resource] / European Union Agency for Network and Information Security (ENISA). 2015. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2014 (Дата обращения 4.04.2016)

Обладая самой новейшей информацией, ENISA способно разработать общий механизм обеспечения защиты инфраструктуры государств-членов Европейского союза, что было бы хорошим результатом работы агентства. Общий механизм с учетом особенностей каждого государства будет лучше и быстрее поддаваться анализу, а следовательно, ENISA сможет быстрее реагировать на новые угрозы и помогать в их нейтрализации. Кроме того, в будущем ENISA необходимо больше вовлечь частный сектор в работу по киберсфере, например, в организацию кибер учений – подобный интерес со стороны коммерческих предприятий показал бы, что общий уровень осведомленности о киберсфере среди населения вырос, а значит, Европейский союз будет способен еще лучше сопротевляться угрозам в киберпространстве. В дополнение, ENISA стало пользоваться большим доверием со стороны государственного и частного секторов, о чем, кроме описанного выше, говорит и увеличение объема публикаций – в среднем, с 2014 по апрель 2016 объем публикаций вырос практически в два раза. Хорошим результатом для ENISA стал бы выпуск собственного журнала о кибербезопасности, где, кроме отчетов, докладов и т.д., были бы статьи о кибербезопасности – это помогло бы привлечь еще больше граждан Европейского союза к данной теме, работа которых напрямую не связана с кибербезопасностью, поскольку для них было бы понятнее читать адаптированные статьи об угрозах и способах их предотвращения.

3.3 СОТРУДНИЧЕСТВО ENISA С НЕЕВРОПЕЙСКИМИ ГОСУДАРСТВАМИ И ОРГАНИЗАЦИЯМИ.

Помимо деятельности внутри Европейского союза и сотрудничества с европейскими заинтересованными сторонами, ENISA пытается сотрудничать с международными организациями и иностранными государствами.

Наиболее тесные связи во всех сферах у Европейского союза с Соединенными Штатами, потому ЕС в вопросе безопасного киберпространства больше всего доверял и доверяет США. В 2010 году в рамках саммита ЕС-США[104] через ENISA была образована рабочая группа, которая привела к созданию Атлантических кибер учений, проведенных в 2011 году. В области управления кибер инцидентами, рабочая группа договорилась подготовить программу сотрудничества для синхронизации и координации кибер учений в Европейском союзе и США, которые бы завершились совместными учениями вместе с частными сектором в 2013 году (однако информации о том, что такие киберучения были проведены, найдено не было).[105]

Кроме того, для эффективного управления международными кибер инцидентами, приводящий к кризисам на национальных и международных уровнях, ENISA проводит международные конференции по сотрудничеству и ученям по управлению кибер кризисами - The ENISA International Conferences on Cyber Crisis Cooperation and Exercises, которая помогает ее участникам в построении более последовательной политики в области кибербезопасности. Эти конференции являются важнейшей площадкой для обмена знаниями и практическим опытом между международными экспертами по кибербезопасности. На данный момент было организовано две конференции – в 2012 и 2013 годах.

---

104 EU-US WORKING GROUP ON CYBER-SECURITY AND CYBER-CRIME. Concept Plan [Electronic resource] / ENISA. 2011. URL: http://www.statewatch.org/news/2011/apr/eu-us-2011-04-13-concept-paper-cybersecurity.pdf (Дата обращения 6.04.2016)

105 The Foreign Policy of the European Union Assesing Europe's Role in the World. Second Edition / Bindi F., Angelecu I. – Washington: Brookings Institution Press, 2012. – p. 225

На первой конференции рассматривались вопросы, связанные больше с организацией, планированием и управлением кибер учениями.[106] Вторая же конференция была больше посвещена таким вопросам, как сбор информации о текущем положении дел, международным кибер учениям, обсуждению механизмов по обмену данными и взаимодействию и так далее. Помимо европейских государств и организаций, в ней принимали участие, в основном, представители американской стороны.[107] Таким образом, можно сделать вывод, что ENISA и Европейский союз в целом больше внимания уделяют двустороннему сотрудничеству с США, чем глобально международному. Возможно это связано с тем, что именно США и Европейские государства на данный момент обладают самыми передовыми знаниями об информационных технологиях. Хотя на последней конференции было сделано предложение о том, что нужно провести третью встречу в неевропейском государстве и сфокусироваться именно на международном сотрудничестве[108], но скорее всего, в таком случае встреча будет проведена в США.

На данный момент, ENISA практически не вовлечена в международное сотрудничество вне европейского союза, в ее многолетнем плане до 2017 года даже не упоминается такая задача, как развитие сотрудничества с неевропейскими государствами и организациями. Иногда, как мы видим выше, ENISA организовывает мероприятия консультативного характера, в которых, помимо государств-членов ЕС и европейских агентств и организаций, принимают участие лишь представители Соединенных Штатов Америки. Однако, данное исследование показывает, что ENISA с каждым годом увеличивает свое значение по обеспечению кибербезопасности, все больше иностранных государств и организаций обращаются к материалом агентства и используют их, что говорит нам о положительной тендеции для развития организации в будущем.

---

106 1st International Conference on Cyber Crisis Exercices & Cooperation. Information Package [Electronic resource] / ENISA. 2012. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/conference/cyber-exercise-conference/info-pkg (Дата обращения 6.04.2016) p. 14

107 2nd International Conference on Cyber-crisis Cooperation and Exercises. Participant information package [Elecronic resource] / ENISA. 2013. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/conference/2nd-enisa-conference/infopkg (Дата обращения 6.04.2016) p. 23-30

108 Report on Second International Conference on Cyber-crisis Cooperation and Exercises [Electronic resource] / ENISA. 2013. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/conference/2nd-enisa-conference/report (Дата обращения 6.04.2016) p.13

Если говорить в целом, то известно, что большинство европейских государств обладают достаточным количеством ресурсов и знаний, чтобы стать передовым организатором международного глобального сотрудничества, поскольку в нем есть острая необходимость – киберугрозы трансграничны, поэтому между государствами должны существовать четкие договоренности о том, как поступать в случае транснациональных кибер инцидентов. ENISA способно стать источником законадательных инициатив для международного права в области кибербезопасности, учитывая свой многолетний опыт, материалы и наличие передовых европейских экспертов в данной сфере. Это существенно бы повысило уровень Европейского союза на международной арене в данной области, поскольку рекомендации агентства становились бы законодательными актами. Превратиться в международную организацию ENISA не суждено, поскольку такой орган у ж е существует – специальное учреждение при Организации Объединенных Наций Международный союз электросвязи (International Telecommunication Union)[109]. И как раз через него ENISA могло бы привносить законодательные инициативы, но для этого в агентстве должен быть создан орган, который будет отвечать за развитие международного сотрудничества (не только с США, но и с другими государствами). Кроме того, ENISA обладает необходимым опытом и возможностью помогать в организации крупных международных киберучений.

109 About ITU [Electronic resource] / ITU. URL: http://www.itu.int/en/about/Pages/default.aspx (Дата обращения 6.04.2016)

ЗАКЛЮЧЕНИЕ

Киберпространство – неоднородная среда, которая не обладает физической оболочкой, но нуждается в пристальном внимании и постоянной защите. Европейский союз для данной цели создал агентство по сетевой и информационной безопасности, которое собирает информацию о кибер инцидентах, анализирует ее, выпускает рекомендации по преодолению различного вида киберугроз и помогает государствам, организациям и гражданам Европейского союза в их предотвращении. ENISA в 2020 году должно получить следующий мандат, который будет продлен только в случае успешного функционирования агентства. Данное исследование ставило перед собой цель установить эффективность работы агентства и спрогнозировать возможный сценарий его развития в будущем.

Первая задача заключалась в определении ключевых терминов по вопросу киберпространства и кибербезопасности. Разработка четкого понятийного аппарата важна для грамотного понимания данной области. Проанализировав ряд статей по кибербезопасности и тематические новостные издания, данное исследование смогло выработать свое определение киберпространства как трудной для понимания среды, не обладающей физической формой, созданной путем взаимодействия людей, программного обеспечения и Интернета с помощью электричества, специального оборудования и сетей, связанных с ними.

Для понимания того, в каком направлении агентство планирует двигаться, необходимо было выполнить *вторую задачу* исследования – обозначить исторические причины создания ENISA, ее цели и задачи, то есть разобрать основу агентства. Исходя из анализа нескольких уставов (первоначального, дополнений к нему и нового), а также проанализировав рабочие программы за 2014-2016 года, был сделан вывод о том, что на агентство с каждым годом возлагаются все более ответственные и сложные задачи. Это позволило предположить возможность для агентства серьезно расширить свои полномочия в будущем.

Кроме того, на эффективность работы организации напрямую влияет ее внутреннее устройство, именно поэтому требовалось выполнение *третьей задачи* исследования: дать

оценку эффективности внутренней организации работы. За годы работы агентства его структура менялась несколько раз. Изначально у исполнительного директора было множество помощников и департаментов по работе в прямом подчинении, что существенно осложняло контроль. На сегодняшний момент исполнительный директор имеет личного помощника и взаимодействует с главами двух департаментов, которые в свою очередь выстраивают работу в своих отделах. Данная реорганизация позволяет намного быстрее и эффективнее принимать решения.

Четвертой задачей являлось обозначение критериев оценки эффективности работы агентства. Для данного исследования первостепенную роль сыграли такие показатели, как увеличение финансирования агентства (в 2016 году объем финансирования вырос практически на 1 000 000 евро по сравнению с 2014 годом), появление все более сложных задач, увеличение востребованности научными статьями ENISA со стороны иностранных организаций и государств на 2016 год, увеличение общего объема научных публикаций, успешные ежегодные проекты (например, европейский месяц кибербезопасности), в которых принимают участие множество специалистов. Однако минусом стало практические полное отсутсвие взаимодействия с неевропейскими государствами.

Последней задачей являлось выявление факторов для построения сценария будущего развития ENISA. Данное исследование определило для себя, что ENISA необходимо больше вовлекаться в международную деятельность за пределами Европейского союза. Единственным зарубежным участником встреч, конференций, проводимых агентством, являются представители США. Совместные проекты тоже проводились только с ними. Поэтому сделан вывод о том, что ENISA необходимо больше внимания уделять мировому развитию кибербезопасности, в частности, например, с помощью законодательных инициатив для международного права в киберпространстве, которые можно было бы воплощать в жизнь через специальное подразделение ООН или с помощью организации международных киберучений.

Кроме того, есть необходимость в вовлечении частного сектора в развитие кибербезопасности. Данное исследование показало, что в практическую деятельность агентства еще слишком мало вовлечен частный сектор: например, практически все киберучения проводятся государствами, но не частными организациями. И этому стоит уделить внимание, поскольку вовлеченность частного сектора существенно повысит осведомленность граждан ЕС о киберугрозах и способах борьбы с ними, а, следовательно,

повысит общий уровень безопасности. Кроме того, осведомленность граждан по данному вопросу повысил бы выпуск собственного журнала агентства, в котором были бы и статьи для технических специалистов, и адаптированные статьи под рядовых пользователей без особых знаний.

Более того, выше было обозначено, что на агентство с каждым годом возлагают все более ответственные задачи, что позволяет предположить возможное расширение его полномчий. В частности, учитывая, что агентство оказывает поддержку государствам Евросоюза в улучшении национальных стратегий кибербезопасности (НСК), оно могло бы анализировать существующие стратегии и оставлять их в публичном доступе для того, чтобы другие государства Европейского союза могли на них ориентироваться. Это привело бы к усилению кибербезопасности всего Европейского союза в целом. В дополнение, ENISA, учитывая свой уже 12-летний опыт и наличие профессиональной команды экспертов в сфере информационной безопасности со всех стран Европейского союза, могло бы разработать общий механизм защиты важнейших государственных инфраструктур в странах – членах ЕС, что позволило бы агентству быстрее и успешнее анализировать происходящие кибер инциденты и реагировать на них, поскольку общий механизм будет им хорошо знаком.

Цель данного исследования была полностью достигнута: согласно результатам, агентство по сетевой и информационной безопасности приносит огромную пользу для развития и поддержания кибербезопасности в Европейском союзе и является высокоэффективным быстроразвивающимся европейским институтом с большими возможностями. Прежде всего, ENISA помогает развивать национальные стратегии по кибербезопасности государств ЕС; кроме того, ежегодно проводит мероприятия по кибербеопасности и помогает в организации внутрегосударственных кибер учений; в дополнение, объем научных публикаций ENISA постоянно растет, и к ним все чаще обращаются иностранные организации при развитии собственных механизмов по кибербезопасности; кроме того, ENISA тестно сотрудничает с представителями США в данной сфере, однако другие неевропейские государства в кибер учениях пока что не участвуют. Скорее всего, в будущем вектор работы ENISA будет направлен на дальнейшее развитие внутренней кибербезопасности Европейского союза и развитие международных отношений в этой сфере через взаимодействие, прежде всего, с иностранными крупными организациями.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

ИСТОЧНИКИ

1. 1st International Conference on Cyber Crisis Exercices & Cooperation. Information Package [Electronic resource] / ENISA. 2012 .URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/conference/cyber-exercise-conference/info-pkg (Дата обращения 10.04.2016)
2. 2nd International Conference on Cyber-crisis Cooperation and Exercises. Participant information package [Elecronic resource] / ENISA. 2013. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/conference/2nd-enisa-conference/infopkg (Дата обращения 10.04.2016)
3. Acts adopted unser title VI of the EU treaty council decision establishing the European Police Office (Europol) [Electronic resource] / Official Journal of the European Union. 2009. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:121:0037:0066:en:PDF (Дата обращения 10.04.2016)
4. Amending Statement of Estimates no 01/2015 (Amending Budget 2015) [Electronic resource] / European Union Agency for network and information security. 2015. URL: https://www.enisa.europa.eu/about-enisa/accounting-finance/files/annual-budgets/amending-budget-1-2015-final (Дата обращения 10.04.2016)
5. Amending Statement of Estimates no 02/2014 (Amending Budget no 02/2014) [Electronic resource] / European Union Agency for network and information security. 2014. URL: https://www.enisa.europa.eu/about-enisa/accounting-finance/files/annual-budgets/enisa-amending-budget-2-2014 (Дата обращения 10.04.2016)
6. An evaluation Framework for National Cyber Security Strategies [Electronic resource] / European Union Agency for Network and Information Security. 2014. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1 (Дата обращения 10.04.2016)
7. Annual Activity Report 2014. [Electronic resource] / ENISA. Publications Office of the European Union. 2014. URL: https://www.enisa.europa.eu/publications/programmes-reports/enisa-annual-activity-report-2014 (Дата обращения 10.04.2016)

8. Annual Incident Reports 2014: Analysis of Article 13a annual incident reports [Electronic resource] / European Union Agency for Network and Information Security (ENISA). 2015. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2014 (Дата обращения 10.04.2016)
9. Convention on cybercrime [Electronic resource] / Council of Europe Budapest. 2001. URL: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (Дата обращения 10.04.2016)
10. Cyber Europe 2012: Key Findings Report [Electronic resource] / ENISA. 2012. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/cyber-europe-2012/cyber-europe-2012-key-findings-report (Дата обращения 10.04.2016)
11. Cyber Security Report [Electronic resource] / European Commission. 2013. URL: http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf (Дата обращения 10.04.2016)
12. Cyber Security Report [Electronic resource] / European Comission. 2015. URL: http://ec.europa.eu/COMMFrontOffice/PublicOpinion/index.cfm/Survey/getSurveyDetail/yearFrom/1973/yearTo/2016/search/cyber/surveyKy/2019 (Дата обращения 10.04.2016)
13. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. [Electronic resource] / High Representative of the European Union for Foreign Affairs and Security Policy. Brussel, 2013. URL: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf (Дата обращения 10.04.2016)
14. Decision No MB/2014/1 WP Of the Management Board of the European Union Agency for Network and Information Security (ENISA) The financial regulation applicable to the European Union Agency for Network and Information Security in conformity with the Commission Delegated Regulation (EU) No 1271/2013 of 30 September 2013 on the framework financial regulation for the bodies referred to in Article 208 of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council [Electronic resource] / ENISA. 2014. URL: https://www.enisa.europa.eu/about-enisa/accounting-finance/files/enisa-financial-regulation-1 (Дата обращения 10.04.2016)
15. Decision No MB/2014/7 of the Management Board of the European Union Agency for Network and Information Security on the establishment and operation of the Permanent Stakeholders' Group [Electronic resource] / ENISA. 2014. URL: https://www.enisa.europa.eu/about-enisa/structure-organization/management-

board/management-board-decisions/mb-decision-no-mb-2014-7-on-internal-rules-of-operation-of-psg (Дата обращения 10.04.2016)

16. Draft Council Conclusions on the Renewed European Union Internal Security Strategy 2015-2020 [Electronic resource] / Council of the European Union. 2015. URL: http://statewatch.org/news/2015/jun/eu-council-iss-draft-conclusions-9416-15.pdf (Дата обращения 10.04.2016)

17. EU-US WORKING GROUP ON CYBER-SECURITY AND CYBER-CRIME. Concept Plan [Electronic resource] / ENISA. 2011. URL: http://www.statewatch.org/news/2011/apr/eu-us-2011-04-13-concept-paper-cybersecurity.pdf (Дата обращения 10.04.2016)

18. Evaluation of the European Network and Information Security Agency [Electronic resource] / Experts Panel IDC EMEA. 2007. URL: http://ec.europa.eu/smart-regulation/evaluation/search/download.do;jsessionid=rpwq5oEp3UR9t_KpFpSEG2Sq2uVnPh0EwEj3aYj2vxrIRun8DRRA!1168777535?documentId=814 (Дата обращения 10.04.2016)

19. Finland´s Cyber security Strategy [Electronic resource] / Finland. : Forssa print, 2013. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/FinlandsCyberSecurityStrategy.pdf (Дата обращения 10.04.2016)

20. General report 2005 [Electronic resource] / European Network and Information Security Agency. Brussels. 2005. URL: https://www.enisa.europa.eu/publications/programmes-reports/enisa_work_programme_2005.pdf (Дата обращения 10.04.2016)

21. General report 2008 [Electronic resource] / European Network and Information Security Agency. 2009. URL: https://www.enisa.europa.eu/publications/programmes-reports/enisa_gr_2008.pdf (Дата обращения 10.04.2016)

22. Kroes N. Speech : EU Cyber Security Strategy. [Electronic resource] / Davos. 2013. URL: http://europa.eu/rapid/press-release_SPEECH-13-51_en.html (Дата обращения 10.04.2016)

23. National Cybersecurity Strategy [Electronic resource] / Spain. 2013 URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS_ESen.pdf (Дата обращения 10.04.2016)

24. National Strategy to Secure Cyberspace [Electronic resource] / USA. 2003. URL: http://www.dhs.gov/national-strategy-secure-cyberspace (Дата обращения 10.04.2016)

25. On National and International Cyber Security Exercises: Survey, Analysis and Recommendations [Electronic resource] / European Network and Information Security Agency (ENISA). 2012. URL: https://www.enisa.europa.eu/activities/Resilience-and-

CIIP/cyber-crisis-cooperation/cce/cyber-exercises/exercise-survey2012 (Дата обращения 10.04.2016)

26. Regulation (EC) No 460/2004 the European Parliament and of the Council. Establishing the European Network and Information Security Agency [Electronic resource] / Official Journal of the European Union. 2004. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004R0460 (Дата обращения 10.04.2016)

27. Regulation (EU) No 526/2013 of the European Parlament nd of the council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 [Electronic resource] / Official Journal of the European Union. 2013. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:JOL_2013_165_R_0041_01&qid=1397226946093&from=EN (Дата обращения 10.04.2016)

28. Regulation (EU) No 910/2014 of the European parlament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [Electronic resource] / Official Journal of the European Union. 2014. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG (Дата обращения 10.04.2016)

29. Regulation (EC) No 1007/2008 the European Parlament nd of the council of Establishing the European Network and Information Security Agency as regards its duration: amending Regulation (EC) No 460/2004 [Electronic resource] / Official Journal of the European Union. 2008. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2008.293.01.0001.01.ENG (Дата обращения 10.04.2016)

30. Report on Second International Conference on Cyber-crisis Cooperation and Exercises [Electronic resource] / ENISA. 2013. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/conference/2nd-enisa-conference/report (Дата обращения 10.04.2016)

31. The European Cyber Security Month 2015: Deployment report [Electronic resource] / European Union Agency for Network and Information Security (ENISA). 2015. URL: https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign/2015 (Дата обращения 10.04.2016)

32. United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union / the Court of Justice of the European Union. 2004. URL:

http://curia.europa.eu/juris/showPdf.jsf;jsessionid=9ea7d2dc30db8ba88b5908ff47d6961c9f441c2ac18d.e34KaxiLc3qMb40Rch0SaxuKaNr0?docid=57031&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=5545180 (Дата обращения 10.04.2016)

33. Work programme 2014 [Electronic resource] / ENISA. 2013. URL: https://www.enisa.europa.eu/publications/programmes-reports/work-programme-2014 (Дата обращения 10.04.2016)

34. Work Programme 2015 Including Multi-Annual Planning [Electronic resource] / the European Union Agency for Network and Information Security. 2014. URL: https://www.enisa.europa.eu/publications/programmes-reports/enisa-work-programme-2015 (Дата обращения 10.04.2016)

35. Work programme 2016 Including multiannual planning [Electronic resource] / European Union Agency for Network and Information Security. 2015. URL: https://www.enisa.europa.eu/publications/programmes-reports/enisa-work-programme-2016 (Дата обращения 10.04.2016)

ЛИТЕРАТУРА

1. *Владимирова Т. В.* Об обеспечении информационной безопасности в условиях кибепространства // Вопросы безопасности. – 2014. №3. – С. 132-157
2. *Владимирский А.* Европейский парламент дает «зеленый свет» Агентству ENISA на реализацию Стратегии кибербезопасности ЕС [Электронный ресурс] / Экспертный центр электронного государства. 2013. URL: http://d-russia.ru/evropejskij-parlament-daet-zelenyj-svet-agentstvu-enisa-na-realizaciyu-strategii-kiberbezopasnosti-es.html (Дата обращения 10.04.2016)
3. *Добродеев А.Ю., Бородакий Ю. В., Бутусов И.В.* Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1) // Вопросы кибербезопасности. – 2013. №1.- С. 2-9
4. Информационное общество и международные отношения / К. А. Панцерев [и др.], под ред. К.А. Панцирева. – СПб.: изд-во СПбГУ, 2014. – 384 с.

5. *Панцерев К. А*. Современные модели информационного общества: типологическая характеристика // Вестник Санкт-Петербургского университета. Серия 6. Политология. Международные отношения. – 2011. №1. С. 39-45
6. *Петренко А.А, Петренко С. А*. Киберучения: методические рекомендации ENISA // Вопросы кибербезопасности – 2015. №3(11) – С. 2-14
7. Словарь-справочник терминов в области кибербезопасности / авт.-сост. Воронков И.М. и др - М.: Сам полиграфист, 2014. – С. 229
8. Уэбстер Ф. Теории информационного общества / - М.: Аспект Пресс, 2004. – 400 с.
9. *Clark D.* Characterizing cyberspace: past, present and future. [Electronic resource] / MIT CSAIL. 2010. URL: http://web.mit.edu/ecir/pdf/clark-cyberspace.pdf (Дата обращения 10.04.2016)
10. *Jozef Vyskoč, Zsolt Illési, Joanna Świątkowska, Tomáš Rezek* Protecting cyberspace in the V4: Towards implementation of the EU's cyber-security strategy [Electronic resource] / Central European Policy Institute. 2013. URL: http://www.cepolicy.org/publications/protecting-cyberspace-v4-towards-implementation-eus-cyber-security-strategy (Дата обращения 10.04.2016)
11. New EU Cybersecurity strategy & Directive announced [Electronic resource] / ENISA. 2013. URL: https://www.enisa.europa.eu/media/news-items/new-eu-cybersecurity-strategy-directive-announced (Дата обращения 10.04.2016)
12. New Regulation for EU cybersecurity agency ENISA, with new duties [Electronic resource] / ENISA. 2013. URL: https://www.enisa.europa.eu/media/press-releases/new-regulation-for-eu-cybersecurity-agency-enisa-with-new-duties (Дата обращения 10.04.2016)
13. The Foreign Policy of the European Union Assesing Europe's Role in the World. Second Edition / Bindi F., Angelecu I. – Washington: Brookings Institution Press, 2012. – P. 369

ПРИЛОЖЕНИЕ

Приложение 1.

Частота использования интернета жителями Евросоюза, Сравнительный анализ за 2013-2014 года на основе репортов о кибербезопасности.

Использование Интернета	Год	Каждый день	Около 2-х раз в неделю	Около 2-х раз в месяц	Никогда	Нет доступа в интернет
Дома	2014	60%	8%	1%	17%	9%
	2013	54%	10%	1%	20%	10%
На работе	2014	29%	4%	1%	49%	13%
	2013	24%	4%	1%	52%	16%
В других места (университет, интернет кафе и т.д.)	2014	16%	5%	2%	56%	10%
	2013	9%	5%	2%	65%	9%

ПРОЦЕНТ СНИЗИЛСЯ ПРОЦЕНТ ВЫРОС

ПРИЛОЖЕНИЕ 2.

Сравнительная таблица онлайн-активности граждан Евросоюза, по материалам репортов о кибербезопасности за 2013-2014 года (предполагалась возможность выбора нескольких вариантов).

Использование социальных сетей	2014	60%
	2013	53%
Покупка товаров и услуг онлайн	2014	57%
	2013	50%
Использование услуг интернет-банка	2014	54%
	2013	48%
Продажа товаров и услуг онлайн	2014	23%
	2013	18%

ПРИЛОЖЕНИЕ 3

Сравнительная таблица ответов граждан ЕС на основе репортов о кибербезопасности за 2013-2014 года. (Предполагалось согласие/частичное согласие/несогласие с поставленным заявлением)

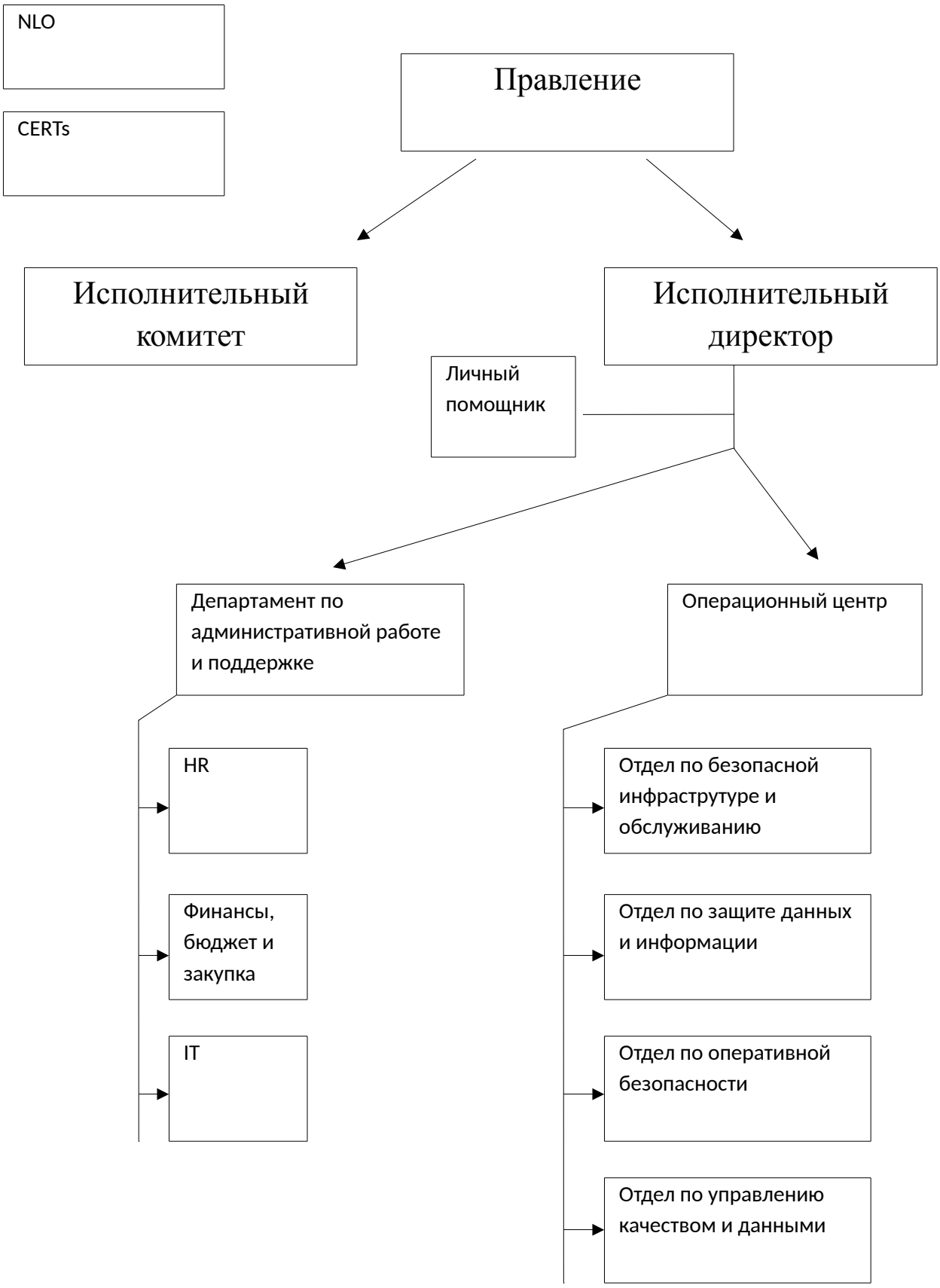
Утверждение	Год	Согласен	Частично согласен	Не согласен	Не знаю
Я беспокоюсь, что персональная информация обо мне недостаточно защищается <u>вебсайтами</u>	2014	30%	61%	6%	3%
	2013	26%	66%	5%	3%
Я беспокоюсь, что моя персональная информация недостаточно защищается <u>правительством</u>	2014	27%	62%	8%	3%
	2013	23%	67%	7%	3%

ПРИЛОЖЕНИЕ 4

Сравнительная таблица граждан Евросоюза, отвечавших на вопрос об информированности по поводу киберугроз, сделанная на основе репортов о Кибербезопасности за 2013-2014 года

Насколько вы знакомы с киберугрозами?					
Год	**Очень хорошо**	**Хорошо**	**Не очень знаком**	**Немного знаком**	**Не знаю**
2013	9%	35%	29%	23%	4%
2014	10%	37%	29%	21%	3%

ПРИЛОЖЕНИЕ 5



ПРИЛОЖЕНИЕ 6

Общие расходы по деятельности, согласно рабочей программе ENISA 2014

№	Название	Затраты на зарплату (евро)	Затраты на деятельность (евро)	Накладные расходы (евро)	
1	помощь в построение европейского политики	708 981	280 000	844 376	
2	Поддержка в построении возможностей	958 293	495 000	1 141 300	
3	Поддержка сотрудничества	1 071 054	459 000	1 275 594	
4	Миссии	0	500 000	0	
1	Отношения заинтересованных сторон (работа секретариатов, поддержка связи с институтами ЕС)	152 559	260 000	181 693	
2	Корпоративная коммуникация	152 559	50 000 евр	181 693	
3	Деятельность по поддержке проектов	152 559	40 000	181 693	
	Итого:	3 196 005	2 084 000	3 806 349	9 086 354