Анатолий А. Малюк, Ольга Ю. Полянская
Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
e-mail: AAMalyuk@mephi.ru, https://orcid.org/0000-0002-5746-1508,
e-mail: OYPolyanskaya@mephi.ru, https://orcid.org/0000-0001-9867-3278

ОПЫТ РЕАЛИЗАЦИИ ПИЛОТНОГО ПРОЕКТА ЕВРОПЕЙСКОЙ СИСТЕМЫ ОПОВЕЩЕНИЯ И ОБМЕНА ИНФОРМАЦИЕЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*

DOI: http://dx.doi.org/10.26583/bit.2018.1.01

Аннотация. Формирование глобального информационного общества с особой остротой ставит проблему развития культуры информационной безопасности. В Доктрине информационной безопасности Российской Федерации, принятой в декабре 2016 года, как одна из основных угроз определяется низкая осведомленность граждан в вопросах обеспечения личной информационной безопасности.

Одним из наиболее важных механизмов повышения компетентности и формирования культуры информационной безопасности, помимо массового обучения людей, являются методы пропаганды и создания «горячих линий». Они позволяют широкой общественности брать на себя инициативу в наблюдении и уведомлении о компьютерных инцидентах. Развитие подобных подходов целесообразно осуществлять с учетом накопленного сегодня международного опыта.

С этой целью в статье рассматривается европейский опыт создания системы информационно-консультативной помощи в области предупреждения угроз безопасности использования общедоступных и корпоративных информационных систем, а также ликвидации последствий проявления угроз в информационной сфере. Анализ опыта реализации пилотного проекта европейской системы оповещения и обмена информацией выявил целесообразность проектирования подобных систем на основе модели управления с четырьмя игроками, объединяющей операторов сети, производителей информации (которые являются поставщиками ИТ-продуктов или специалистами в области ИТ-безопасности), локальных информационных посредников и потребителей информации. В качестве модели информационного потока может быть выбран узел, который запускает локальный веб-портал, предоставляющий информацию для конечных пользователей, формирует новую информацию, адаптирует информацию к ограничениям различных каналов распространения и к характеристикам целевых групп конечных пользователей. Методология пилотного проекта может быть использована при проектировании и развертывании системы оповещения и обмена информацией, ориентированной на конечных пользователей нескольких регионов или стран, сотрудничающих в области информационной безопасности.

Ключевые слова: информационная безопасность, осведомленность по вопросам информационной безопасности, система оповещения и обмена информацией, культура информационной безопасности.

Для цитирования. ***МАЛЮК, Анатолий А.; ПОЛЯНСКАЯ, Ольга Ю.*** *ОПЫТ РЕАЛИЗАЦИИ ПИЛОТНОГО ПРОЕКТА ЕВРОПЕЙСКОЙ СИСТЕМЫ ОПОВЕЩЕНИЯ И ОБМЕНА ИНФОРМАЦИЕЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Безопасность информационных технологий, [S.l.], v. 25, n. 1, p. 6-18, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1089>. Дата доступа: 14 feb. 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.01.*

* ***Благодарности.*** Работа выполнена при финансовой поддержке РФФИ (отделение общественных и гуманитарных наук), проект № 15-03-00248: Проведение научных исследований по направлению «Формирование в обществе культуры информационной безопасности».

Anatoly A. Malyuk, Olga Y. Polyanskaya
National Nuclear Research University MEPHI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia
e-mail: AAMalyuk@mephi.ru, https://orcid.org/0000-0002-5746-1508,
e-mail: OYPolyanskaya@mephi.ru, https://orcid.org/0000-0001-9867-3278

Experience of the pilot implementation of the european information sharing and alerting system in the field of information security*

DOI: http://dx.doi.org/10.26583/bit.2018.1.01

Abstract. The formation of a global information society poses a particular challenge to the development of an information security culture. In the Doctrine of Information Security of the Russian Federation, adopted in December 2016, one of the main threats is the low awareness of citizens in matters of ensuring personal information security.
One of the most important mechanisms for increasing competence and forming an in-formation security culture, in addition to mass training of people, are methods of propaganda and creation of "hot lines". They allow the general public to take the initiative in monitoring and reporting computer incidents. The development of such approaches should be carried out taking into account the international experience accumulated today.
To this end, the article examines the European experience of creating a system of information and advisory assistance in the field of preventing threats to the security of public and corporate information systems, primarily information and telecommunications networks, as well as eliminating the consequences of threats in the information sphere. The analysis of the experience of implementing the pilot project of the European Information Sharing and Alert System has revealed the advisability of designing such systems on the basis of a management model with four players that unites network operators, information producers (who are IT product suppliers or IT security specialists); local information intermediaries and consumers of information. As a model of the information flow, a node can be selected that runs a local web portal that provides information to end users, generates new information, adapts information to the constraints of various distribution channels, and to the characteristics of end-user target groups. The methodology of the pilot project can be used in the design and deployment of a notification and information exchange system aimed at end-users of several regions or countries cooperating in the field of information security.

Keywords: information security, information security awareness, information sharing and alerting system, culture of information security.
For citation. ***MALYUK, Anatoly A.; POLYANSKAYA, Olga Y.*** *Experience of the pilot implementation of the european information sharing and alerting system in the field of information security. IT Security (Russia), [S.l.], v. 25, n. 1, p. 6-18, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1089>. Date accessed: 14 feb. 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.01.*

* ***Acknowledgements:*** This research was executed at financial support of RFBR (Department of social Sciences and Humanities), project No. 15-03-00248: Conducting research in the field of "Formation of a culture of information security"

Введение

Развитие глобального информационного общества выдвигает на передний план задачу формирования специфических общественных отношений и новых форм межличностного и корпоративного взаимодействия. Особенно это касается вопросов обеспечения личной, общественной и государственной безопасности. Новизна поставленной задачи определяется тем, что в настоящее время недостаточно научных работ по принципам формирования культуры информационной безопасности, особенно в России.

По мнению авторов многих научных статей в этой области [1-4], формирование в обществе культуры информационной безопасности предполагает, прежде всего, создание

механизмов, с помощью которых государство может повлиять на процессы развития информационного общества и перейти от декларации основных направлений политики в этой сфере к разработке конкретных программ и массовому обучению широких слоев пользователей. Среди первоочередных задач эксперты в своих работах [5-9] выделяют следующие: расширение вклада средств массовой информации в пропаганду культуры информационной безопасности, совершенствование типовых норм по обеспечению безопасности использования общедоступных и корпоративных информационных систем и информационно-телекоммуникационных сетей, реализация системы массового обучения в области культуры информационной безопасности с использованием возможностей глобальных информационно-телекоммуникационных сетей, разработка основных образовательных программ по формированию культуры информационной безопасности.

В этом перечне задач, как отмечается в ряде работ [10-15], одно из главных мест занимают вопросы создания системы информационно-консультативной помощи в области предупреждения угроз безопасности использования общедоступных и корпоративных информационных систем, в первую очередь информационно-телекоммуникационных сетей, а также ликвидации последствий проявления угроз в информационной сфере. Представляется, что основное внимание при организации такой информационно-консультативной помощи должно быть сосредоточено на ряде следующих ключевых проблем:

- создание порталов и сайтов, содействующих оказанию информационно-консультативной помощи пользователям общедоступных и корпоративных информационных систем, и информационно-телекоммуникационных сетей;
- разработка и реализация перспективных проектов негосударственных организаций, направленных на оказание информационно-консультативной помощи;
- совершенствование правовых механизмов организации широкого обмена информацией и взаимодействия на международном уровне в целях предотвращения новых угроз, приобретающих трансграничный характер;
- совершенствование взаимодействия уполномоченных государственных органов на международном уровне.

На сегодняшний день большой практический интерес представляет зарубежный (прежде всего, европейский) опыт создания такого рода систем информационно-консультативной помощи, который и является предметом дальнейшего нашего рассмотрения.

1. История вопроса (проект FISHA)

До начала 2000-х годов развитые европейские государства не были обеспокоены отсутствием у граждан знаний в области сетевой и информационной безопасности, знаний о том, что такое риски и угрозы в этой сфере и как защитить себя от них. Но, в конце концов, в странах ЕС появилось понимание, что без определенной культуры и надлежащего в смысле информационной безопасности поведения граждане и представители малых и средних предприятий, пользующиеся ИКТ-устройствами, подключенными к Интернету, представляют угрозу для критически важных информационных инфраструктур своих стран. Многие эксперты [16-20] полагают, что без определенного уровня подготовки и информированности работников по вопросам информационной безопасности невозможно обеспечить культуру безопасности в организациях. Основой для формирования культуры информационной безопасности в развитых странах стали рекомендации и аналитические материалы Организации экономического сотрудничества и развития (ОЭСР) [15, 21-23], а также документы и резолюции Европейской комиссии и Европейского Союза [24-26, 28]. В ряде документов [29-32] Европейская комиссия признала важность глобальных мер по повышению уровня информированности домашних пользователей и представителей малых и средних предприятий (МСП) по вопросам информационной безопасности и отвела в этом деле ключевую роль государствам-членам ЕС. В целях повышения европейского потенциала

реагирования на сетевые угрозы безопасности в 2006 году Комиссия в своей «Стратегии для безопасного информационного общества» предложила создать европейскую систему обмена информацией и оповещения (EISAS – European Information Sharing and Alerting System) [27].

Предполагалось, что система EISAS должна:

- способствовать совершенствованию у всех граждан ЕС, а также представителей МСП знаний и навыков, необходимых для защиты своих ИТ-систем и информационных ресурсов;
- сделать доступной информацию по безопасности для всех европейских граждан и представителей МСП на их родном языке;
- опираться на национальные возможности государств-членов ЕС;
- активизировать сотрудничество между национальными/государственными группами реагирования на компьютерные инциденты CERT в государствах-членах ЕС.

Европейская комиссия обратилась к агентству по сетевой и информационной безопасности Европейского союза ENISA с просьбой «изучить вопрос о целесообразности европейской многоязычной системы по обмену информацией и оповещения» [27]. По инициативе Европейской комиссии был начат рассчитанный на долгое время проект EISAS. Он прошел много этапов от первоначального технико-экономического обоснования в 2007 году до первого крупномасштабного пилотного проекта в 2012 году.

В соответствии с рекомендациями EISAS Roadmap [33] в 2009-2011 годах была разработана Структура для обмена информацией и оповещения FISHA (The Framework for Information Sharing and Alerting). Проект FISHA [34] начался в 2009 году с целью реализации модели EISAS. В центре внимания проекта было три основных направления:

- техническое решение для обмена информацией: P2P-сеть и сеть локальных узлов;
- политическая структура, включающая концепцию распространения информации и рекомендации по созданию устойчивой модели управления;
- план коммуникаций, включающий матрицу коммуникаций и характеристику основных целевых групп для информирования.

В настоящее время известны разные подходы и модели систем обмена информацией по информационной безопасности, описанные в ряде научных работ [35- 41]. Консорциум FISHA предложил модель управления для четырех игроков (модель FISHA) [34]:

- организации сетевой безопасности;
- производители информации;
- локальные информационные посредники (брокеры);
- потребители информации (т.е. граждане и представители МСП).

Организации сетевой безопасности занимали центральное место в этой модели, поскольку они стали бы основными сторонами, заинтересованными в запуске национальных систем оповещения и обмена информацией. К категории организаций сетевой безопасности были отнесены национальные государственные группы реагирования на компьютерные инциденты CERT, а также другие организации, занимающиеся подобной деятельностью в государствах-членах ЕС. Производители информации и информационные посредники, безусловно, считались критически важными субъектами, но выполняли лишь дополнительные функции.

Проект FISHA предложил два вида узлов для управления совместной работой этих игроков: центральный узел и несколько базовых узлов [34]. С точки зрения технического администрирования, организация сетевой безопасности, представляющая центральный узел, помимо всего прочего, должна была нести ответственность за управление сетью базовых узлов. С этой целью в проекте FISHA был разработан прототип веб-приложения (система FISHA), который был основан на технологии P2P для обмена информацией в сети. Центральный узел должен был выполнять функции интерфейса с центральными узлами в других странах. Объединенные виды деятельности, осуществляемые центральным узлом и базовыми узлами, описывались как национальная система оповещения и обмена информацией. Независимо от того являлся ли центральный узел

группой CERT, или нет, эта роль предполагала взятие на себя ответственности за работу и координацию национальной системы оповещения и обмена информацией.

Главным результатом проекта FISHA было создание прототипа веб-приложения для оповещения и обмена информацией. Проект FISHA инициировал создание сети групп информационной безопасности, среди тех национальных/государственных групп CERT, которые согласились предоставлять в стандартном формате информацию по безопасности, обычно используемую для информирования и оповещения конечных пользователей. В принципе, каждая группа CERT использует одни и те же источники информации и подписывается на одни и те же списки рассылки и RSS-каналы для того, чтобы следить за инцидентами безопасности в Интернете в целом. Эти виды деятельности предполагалось разделить между несколькими группами CERT, и таким образом достичь синергетического эффекта. В результате проекта была создана модель прототипа системы, согласно которой группы CERT разделяют эти "объекты информации" и публикуют их на родных языках целевой аудитории – граждан и малого и среднего бизнеса.

Проект FISHA стартовал с деятельности EISAS по сбору, обработке (консолидации и форматированию) и распространению информации (предоставлению информации) в рамках процесса передачи информации, имеющей отношение к безопасности, по сети от источника до конечного пользователя. Ряд экспертов отметили, что система FISHA потенциально может быть очень полезной, если используется для «совместного анализа» информации [34]. Проект FISHA был завершен в 2011 году, доказав правильность концепции. Он предложил совместную техническую платформу для обеспечения эффективного обмена и распространения информации по повышению осведомленности граждан и предприятий малого и среднего бизнеса. В качестве пилотного проекта EISAS система FISHA обеспечивала технические средства для распространения информации по информационной безопасности среди производителей и потребителей информации. Это позволило участникам структуры:

- создать общую базу данных имеющихся материалов для повышения осведомленности по вопросам информационной безопасности;
- просматривать информацию в этой базе данных;
- уведомлять друг друга о недавно появившихся материалах;
- обмениваться общедоступными материалами и участвовать в их создании;
- предоставлять локальным информационным посредникам доступ к локально адаптированным материалам.

ENISA представила план системы EISAS, согласно которому основные функциональные возможности и услуги EISAS должны были быть разработаны и внедрены в виде регионального прототипа EISAS Basic Toolset в 2011 году [42]. Затем этот прототип должен был быть распространен на более крупные сообщества в 2012 году в рамках крупномасштабного пилотного проекта европейской системы обмена информацией и оповещения.

В 2011 году агентство ENISA развило подход EISAS в экспериментальном проекте по повышению информационной осведомленности граждан и предприятий малого и среднего бизнеса в рамках одного государства-члена ЕС. Слабая подготовка и информированность этих целевых групп по вопросам информационной безопасности признается многими авторами [43-47] серьезной угрозой для критически важных информационных инфраструктур многих стран. EISAS Basic Toolset разрабатывался как методология, облегчающая информирование целевых групп EISAS об информационной безопасности и расширяющая их возможности за счет предоставления необходимых средств защиты их компьютеров и информационных активов и помощи в овладении необходимыми навыками [42]. Предполагалось связываться с целевыми группами граждан через предприятия, на которых они работали, и распространять среди них:

- оповещения и предупреждения;
- рекомендации;
- передовые практики и информационно-пропагандистские материалы, в виде

листовок, видео, мультфильмов и т.д.

Технико-экономическое исследование развертывания системы EISAS показало, что, используя подход EISAS Basic Toolset, можно значительно повысить информационную безопасность конечных пользователей и их компьютерного оборудования в домашних условиях [48]. Ключевыми факторами успеха стали информирование конечных пользователей об информационной безопасности в соответствии с их потребностями и пониманием, а также предоставление им структуры поддержки для оказания оперативной помощи в случае необходимости.

2. Реализация основных принципов информирования пользователей

Упомянутый выше подход Basic Toolset определил основу более крупного экспериментального развертывания с участием нескольких государств-членов, которое было осуществлено в виде крупномасштабного пилотного проекта EISAS Large-Scale Pilot, реализованного в 2012 году (это было определено в плане EISAS Roadmap [49]). Крупномасштабный пилотный проект развертывания был сосредоточен на двух основных аспектах: сотрудничестве между соответствующими ключевыми игроками, а также совместной обработке и распространении информации (см. рис. 1). В рамках пилотного проекта EISAS национальные правительственные группы реагирования на компьютерные инциденты CERT и другие подобные сообщества в Германии, Венгрии, Португалии, Норвегии, Испании и Польше объединили усилия с целью повышения информированности домашних пользователей и представителей МСП по вопросам информационной безопасности.

Рис. 1. Роли и виды деятельности участников пилотного проекта (Fig. 1. Roles and activities of participants in the pilot project)

Провайдерами информации были:

- немецкая компания Deutsche Telekom AG (DTAG);
- норвежский центр информационной безопасности NorSIS, государственный орган Норвегии.

В число распространителей информации входили:

- агентство правительства Каталонии, отвечающее за обеспечение безопасности информационно-коммуникационных технологий (ИКТ) CESICAT. (CESICAT также действует как центр реагирования на компьютерные инциденты CERT для каталонского малого и среднего бизнеса, граждан, университетов и органов государственного управления);

- венгерский центр реагирования на компьютерные инциденты CERT Hungary (Biztonsagosinternet hotline);
- польский центр реагирования на компьютерные инциденты CERT Polska;
- одна из крупнейших финансовых организаций Испании la Caixa.

Инновационные информационные материалы были получены от основных участников пилотного проекта. Была создана международная команда для совместной обработки и адаптации материалов к потребностям и особенностям населения каждой из стран-участниц. При поиске и отборе информационных материалов учитывался характер представления материала, поскольку это влияет на его привлекательность для целевой группы населения. Для распространения использовалась высококачественная, предварительно сформированная информация, которая касалась безопасного Интернет-серфинга и ботнетов (веб-справочник), кражи личных данных и фишинга (обучающая викторина), а также и социальной инженерии (интерактивное видео). Все эти материалы распространялись по соответствующим каналам связи (социальные сети, крупные общедоступные веб-сайты, специализированные списки рассылки и т.п.), предназначенным для граждан и представителей малого и среднего бизнеса ЕС.

3. Взаимодействие с участниками информационного общества

Очевидно, что особые условия крупного международного совместного проекта, основанного на добровольной работе разных участников, создавали значительные трудности в управлении проектом (см. табл.1) [50]. Трудности возникали из-за проблем с нахождением «общего языка» (с учетом культуры, часовых поясов, местного контекста, языка общения), а также с координацией групповой работы, мотивацией сотрудников и их готовностью к совместной работе.

Таблица 1. Характеристики взаимодействия участников проекта EISAS Large-Scale Pilot
Table 1. Characteristics of interaction between EISAS Large-Scale Pilot project participants

Влияющие факторы	Количество	Содержание факторов
Страны	6	Дания (2), Германия (11), Греция (2), Венгрия (3), Норвегия (2), Польша (2), Испания и Каталония (3)
Языки	8	каталонский, французский, датский, немецкий, венгерский, норвежский, польский, испанский
Временные зоны	3	GMT+0, GMT+1, GMT+2
Координация групповой работы	Тесная	Планирование выполнения технической настройки, строгое соблюдение последовательности задач (например, программирование выполнялось только после завершения перевода текстов, распространение материалов начиналось только после безошибочного выполнения технической настройки)
Готовность участников к сотрудничеству	Средняя	Отношение к дистанционной коммуникации как к рабочим совещаниям; быстрое установление доверительных отношений
Готовность участников использовать современные технологии для совместной работы	Средняя	Применение традиционных средств коммуникации: электронной почты, конференцсвязи Skype. Платформа управления проектами Web 2.0 использовалась только двумя участниками.

Выводы

Подводя итог, можно констатировать, что на основе трансграничного сотрудничества и государственно-частного партнерства была достигнута цель пилотного проекта EISAS Large-Scale Pilot: шесть различных субъектов в четырех государствах-членах ЕС сотрудничали на постоянной основе в рамках совместной информационно-просветительской кампании. Крупномасштабный пилотный проект работал в течение относительно короткого времени, тем не менее, он позволил выявить ряд факторов, которые необходимо принимать во внимание при развертывании межгосударственной системы обмена информацией и оповещения по вопросам информационной безопасности [50].

Важным фактором в концепции EISAS является наличие материалов по информационной безопасности, которые могут быть использованы для информирования целевых групп. Проект EISAS Large-Scale Pilot ясно продемонстрировал, что участники, готовые предоставить информацию, должны быть поддержаны некоторой структурой центрального управления – информационным посредником, который берет на себя задачу обработки информации после ее получения от поставщика и до ее передачи распространителю, выполняя следующие функции:

- помогает производителям оригинальной информации рекомендациями по поводу создания материалов, распространяемых на международном уровне;
- создает систему стимулов для производителей оригинальной информации, побуждающих их стать поставщиками информации (например, поощряющих государственно-частное партнерство);
- объединяет вместе в команды (группы) партнеров, предоставляющих и распространяющих информацию;
- оказывает услуги по профессиональному переводу и локализации материалов, по решению технических проблем;
- сохраняет передовой опыт, с тем, чтобы со временем отпала необходимость в информационном посреднике.

С учетом затрат времени и усилий участников пилотный проект показал, что координация и посредническая деятельность по обмену информацией между субъектами проекта являются решающими – более 80% работ, необходимых для осуществления EISAS в этом проекте было выполнено информационным посредником [50]. Кроме того, несмотря на то, что трудно было найти высококачественные материалы, пригодные для совместного распространения, именно они являются необходимым условием мотивирования распространителей информации, для того чтобы они взяли на себя необходимую нагрузку по получению материала в Интернете.

Наибольший удельный вес работ пришелся на задачи управления проектом. Управление проектом здесь заключалось не просто в ежедневных административных усилиях по реализации проекта в сжатые сроки, а в поддержании мотивации участников продолжать совместную работу на расстоянии и их убеждении, что стоит идти дальше.

Результаты пилотного проекта свидетельствовали о том, что жизненно важным вопросом в существовании сети EISAS являются устойчивые модели финансирования. Самая большая проблема сотрудничества заключалась в балансе эксплуатационных расходов и стоимости участия в сети. Проект подтвердил, что функционирование EISAS не может быть основано на добровольном участии, особенно тех заинтересованных сторон, основной вид деятельности которых не связан с безопасностью ИКТ. Основным стимулом для участников является предоставление финансовой поддержки. Достаточно высокими оказались расходы на программирование, адаптацию и локализацию информационных материалов [50]. Наиболее затратной по времени активностью в цикле производства информации EISAS была названа обработка имеющейся информации, то есть процесс ее классификации и длительного перевода на европейские языки. Успех EISAS зависит от качества информации, которой обмениваются участники и которая распространяется по целевым группам. Этот показатель должен быть достаточно

высоким, чтобы обеспечить стимулы для участия. Наиболее важным итогом пилотного проекта стало подтверждение того, что система EISAS осуществима в больших масштабах и может быть рекомендована для внедрения по всей Европе.

Результаты этого пилотного проекта свидетельствуют о том, что подход EISAS к европейскому сотрудничеству в области повышения осведомленности в вопросах обеспечения информационной безопасности (и не только, но и в более широком аспекте формирования информационного общества) работает и предлагает экономически эффективное решение для совершенствования знаний и навыков граждан ЕС в условиях постоянно нарастающих киберугроз.

СПИСОК ЛИТЕРАТУРЫ:

1 Малюк А.А., Литинская Л.В., Коваленко С.Ю. Формирование информационной культуры общества – важнейший фактор обеспечения информационной безопасности «Безопасность информационных технологий», вып.4, 2009. сс. 17-24.
2 Ghernouti-Hélie. A National Strategy for an Effective Cybersecurity Approach and Culture. 2010 International Conference on Availability, Reliability and Security, 2010, pp. 370 – 373.
3 Mahfuth Amjad, Yussof Salman, Baker Asmidar Abu, Nor'ashikin Ali. A systematic literature review: Information security culture. 2017 International Conference on Research and Innovation in Information Systems (ICRIIS), 2017, pp.1–6.
4 Martins, A. and Eloff, J. 'Information Security Culture' IFIP TC11 International Conference on Information Security, Cairo, Egypt, 7- 9 May 2002.
5 Малюк, А. А.; Полянская, О. Ю. Зарубежный опыт формирования в обществе культуры информационной безопасности. Безопасность информационных технологий, [S.l.], v. 23, n. 4, p. 25-37, dec. 2016. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/8>. Дата доступа: 12 dec. 2017.
6 Малюк А.А., Полянская О.Ю. Формирование современной культуры информационной безопасности «Инфофорум», журнал «Бизнес и Безопасность в России», октябрь, 2008.
7 Schlienger, T. and S. Teufel 'Analysing Information Security Culture: Increased Trust by an Appropriate Information Security Culture' 14th International Conference on Database and Expert Systems Applications (DEXA 2003), Prague, Czech Republic, September 2003.
8 Schlienger, T. and S. Teufel 'Information Security Culture - From Analysis to Change.' Proceedings of ISSA 2003, Johannesburg, South Africa, 9-11 July 2003.
9 Schlienger, T. and S. Teufel. 'Information Security Culture - The Socio-Cultural Dimension in Information Security Management.' IFIP TC11 International Conference on Information Security, Cairo, Egypt, 7-9 May 2002
10 Alain Esterle, Hanno Ranck, and Burkard Schmitt (edited by Burkard Schmitt). "Information security. A new challenge for the EU". Chaillot Paper no. 76, 2005. [Электронный ресурс] URL: http://www.iss.europa.eu/uploads/media/cp076 .pdf.
11 Popp Robert; Poindexter John. Countering Terrorism through Information and Privacy Protection Technologies. IEEE Security & Privacy. 2006, Volume 4, Issue 6, pp. 18-27.
12 Ryan J. J. C. H. Information security tools and practices: what works? IEEE Transactions on Computers, 2004, Volume: 53, Issue: 8, pp. 1060 – 1063.
13 Schjolberg S., Ghernaouti-Hélie S. A Global Treaty on Cybersecurity and Cybercrime, Second edition, 2011. [Электронный ресурс] URL: http://www.cybercrimelaw.net/documents/.
14 Talib Shuhaili; Clarke Nathan L.; Furnell Steven M. An Analysis of Information Security Awareness within Home and Work Environments. 2010 International Conference on Availability, Reliability and Security, 2010, pp.196-203.
15 The promotion of a culture of security for information systems and networks in OECD countries. [Электронный ресурс] URL: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2005)1/FINAL&docLanguage=En.
16 AlHogail Areej, Mirza Abdulrahman. Information security culture: A definition and a literature review. 2014 World Congress on Computer Applications and Information Systems (WCCAIS), 2014, IEEE, pp.1-7.
17 Ngo L. Zhou, W. Warren, M. Understanding transition towards organizational culture change. Proceedings of the 3rd Australian Information Security Management Conference, Perth Australia, 2005.
18 Ruighaver, A.B. & Maynard, S. Organizational Security Culture: More Than Just an End-User Phenomenon. Proceedings of the 21st IFIP TC-11 International Information Security Conference (IFIP/SEC 2006). May 22, 2006, Karlstad, Sweden, pages 425-430.
19 Ruighaver, A.B., Maynard, S. & S. Chang (2006) Organizational Security Culture: Extending the End-User Perspective. Computers & Security, Volume 26, Issue 1, February 2007, Pages 56-62.
20 Sunthoshan Govender; Elmarie Kritzinger; Marianne Loock. The influence of national culture on information security culture.2016 IST-Africa Week Conference, Year: 2016, pp. 1–9.
21 Cybersecurity policy making at a turning point. Analysing a new generation of national cybersecurity strategies

for the Internet Economy. [Электронный ресурс] URL: http://www.oecd.org/officialdocuments/.
22 OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. [Электронный ресурс] URL: http://www.ftc.gov/bcp/conline/edcams/infosecurity/popups/OECD_guidelines.pdf
23 Summary of responses to the survey on the implementation of the OECD guidelines for the security of information systems and networks: towards a culture of security. [Электронный ресурс] URL: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2003)8/FINAL&docLanguage=En.
24 Commission of the European Communities "Commission Decision of 22 April 2005 establishing the European Research Advisory" Official Journal of the European Union. Board (2005/516/EC), 2005.
25 Commission of the European Communities. "Critical Infrastructure Protection in the Fight against Terrorism" (COM(2004)702). 2004, [Электронный ресурс] Сайт Европейской комиссии. URL: http://europa.eu.int/comm/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf.
26 Commission of the European Communities. "Green Paper on a European Programme for Critical Infrastructure Protection" (COM(2005) 576), 2005. [Электронный ресурс] Сайт Европейской комиссии. URL: http://www.libertysecurity.org/IMG/pdf/EC_-_Green_Paper_on_CI_-_17.11.2005.pdf.
27 Communication: A strategy for a Secure Information Society. 31.05.2006. [Электронный ресурс] Сайт Европейской комиссии. URL: http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=2766 .
28 Council Resolution of 22 March 2007 on a Strategy for a Secure Information Society in Europe. Council of the European Union, Official Journal of the European Union. (C68 /01), 2007. [Электронный ресурс] Сайт Европейского Союза. URL: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/c_068/c_06820070324en00010004.pdf.
29 European Commission Information Society. "Availability and Robustness of Electronic Communication Infrastructures (ARECI) Study". [Электронный ресурс] URL: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/areci_study/index_en.htm .
30 European Commission Justice and Home Affairs. "Freedom, Security and Justice; Protect Infrastructures". [Электронный ресурс] URL: http://ec.europa.eu/justice_home/fsj/terrorism/protection/fsj_terrorism_protection_infrastruct_en.htm.
31 Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection. European Commission Justice and Home Affairs. 2006. [Электронный ресурс] URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006PC0787 :EN:NOT.
32 Network and Information Security: Commission seeks to improve network and information security in Europe. 31.05.2006. [Electronic resource] European Commission. URL: http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=2679.
33 EISAS Roadmap, ENISA, 2011. [Электронный ресурс] Сайт Агентства по сетевой и информационной безопасности Европейского союза (ENISA). URL: https://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap .
34 FISHA project, [Электронный ресурс] Сайт проекта по созданию структуры для обмена информацией и оповещения FISHA (The Framework for Information Sharing and Alerting). URL: http://fisha-project.eu /.
35 Dandurand Luc, Serrano Oscar . Towards improved cyber security information sharing. 2013 5th International Conference on Cyber Conflict (CYCON 2013), IEEE Conference Publications, 2013, pp.1-16.
36 Desourdis Robert I., Contestabile John M. Information sharing for situational understanding and command coordination in emergency management and disaster response. 2011 IEEE International Conference on Technologies for Homeland Security(HST), 2011, pp. 26 – 32.
37 Do Hoang Giang, Ng Wee Keong . Privacy-preserving approach for sharing and processing intrusion alert data. 2015 IEEE Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP). 2015, pp.1-6.
38 Feledi Danie, Fenz Stefan. Challenges of Web-Based Information Security Knowledge Sharing. 2012 Seventh International Conference on Availability, Reliability and Security, 2012, pp.514-521.
39 Holgado Pilar; López de Vergara Jorge E.; Villagrá Víctor A.; Sanz Iván; Amaya Antonio. Sharing information about security alerts using semantic web technologies. 2010 International Conference on Network and Service Management, 2010, pp. 270-273.
40 Ivanc Blaž ; Blažič Borka Jerman. Information Security Aspects of the Public Safety Data Interoperability Network. 2016 European Intelligence and Security Informatics Conference (EISIC), 2016, pp. 88–91.
41 Kokkonen Tero ; Hautamäki Jari, Siltanen Jarmo, Hämäläinen Timo. Model for sharing the information of cyber security situation awareness between organizations. 23rd International Conference on Telecommunications (ICT), 2016, IEEE Conference Publications, pp. 1-5.
42 EISAS Basic Toolset report, ENISA, 2011. [Электронный ресурс] Сайт Агентства по сетевой и информационной безопасности Европейского союза (ENISA). URL: https://www.enisa.europa.eu/publications/eisas-basic-toolset.
43 Bishop M. Education in information security. IEEE Concurrency.2000, Volume 8, Issue 4, pp.4-8.
44 Chia, P. Maynard, S., and Ruighaver, A.B. 'Exploring Organisational Security Culture' Sixth Pacific Asia

Conference on Information Systems, Tokyo, Japan, 2-3 September, 2002.
45 Chia, P. Maynard, S., and Ruighaver, A.B. 'Understanding Organisational Security Culture' in Information Systems: The Challenges of Theory and Practice, Hunter, M. G. and Dhanda, K. K. (eds), Information Institute, Las Vegas, USA, 2003, pp. 335 - 365.
46 Dojkovski, S., Lichtenstein, S and Warren, M. Information Security Culture in Small and Medium Sized Enterprises: A Socio-Cultural Framework, Proceedings of 6th Australian Information Warfare & Security Conference, School of Information Systems, Deakin University, Geelong, Australia, 2005.
47 Dojkovski, S., Lichtenstein, S. and Warren, M. Challenges in Fostering an Information Security Culture in Australian Small and Medium Sized Enterprises, Proceedings of the 5th European Conference on Information Warfare and Security, Academic Conference Limited, United Kingdom, 2006.
48 EISAS Deployment Feasibility Study ENISA, 2013. [Электронный ресурс] Сайт Агентства по сетевой и информационной безопасности Европейского союза (ENISA). URL: http://www.enisa.europa.eu/publications/eisas-deployment-feasibility-study.
49 Network and Information Security: Commission seeks to improve network and information security in Europe. 31.05.2006. [Электронный ресурс] European Commission. URL: http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=2679.
50 EISAS Large-Scale Pilot, Collaborative Awareness Raising for EU Citizens & SMEs ENISA, 2012. [Электронный ресурс] Сайт Агентства по сетевой и информационной безопасности Европейского союза (ENISA). URL: https://www.enisa.europa.eu/.../eisas-large-scale-pilot.

REFERENCES:

[1] Malyuk A.A., Litinskaya L.V., Kovalenko S.Yu. The information culture formation of the society is the most important factor of information security. Bezopasnost' informacionnyh tehnologij (IT Security). ISSN 2074-7128, №.4, 2009, pp. 17-24. (in Russian).
[2] Ghernouti-Hélie. A National Strategy for an Effective Cybersecurity Approach and Culture. 2010 International Conference on Availability, Reliability and Security, 2010, pp. 370 – 373.
[3] Mahfuth Amjad, Yussof Salman, Baker Asmidar Abu, Nor'ashikin Ali. A systematic literature review: Information security culture. 2017 International Conference on Research and Innovation in Information Systems (ICRIIS), 2017, pp.1–6.
[4] Martins, A. and Eloff, J. 'Information Security Culture' IFIP TC11 International Conference on Information Security, Cairo, Egypt, 7- 9 May 2002.
[5] Malyuk, A. A.; Polyanskaya, O. Y.. Foreign experience of the formation of information security culture in society. IT Security (Russia), [S.l.], v. 23, n. 4, p. 25-37, dec. 2016. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/8>. Date accessed: 22 dec. 2017. (in Russian).
[6] Malyuk AA, Polyanskaya O.Yu. Forming a modern culture of information security / «Infoforum», «Biznes i Bezopasnost' v Rossii», October, 2008 (in Russian).
[7] Schlienger, T. and S. Teufel 'Analysing Information Security Culture: Increased Trust by an Appropriate Information Security Culture' 14th International Conference on Database and Expert Systems Applications (DEXA 2003), Prague, Czech Republic, September 2003.
[8] Schlienger, T. and S. Teufel 'Information Security Culture - From Analysis to Change.' Proceedings of ISSA 2003, Johannesburg, South Africa, 9-11 July 2003.
[9] Schlienger, T. and S. Teufel. 'Information Security Culture - The Socio-Cultural Dimension in Information Security Management.' IFIP TC11 International Conference on Information Security, Cairo, Egypt, 7-9 May 2002
[10] Alain Esterle, Hanno Ranck, and Burkard Schmitt (edited by Burkard Schmitt). "Information security. A new challenge for the EU". Chaillot Paper no. 76, 2005. [Electronic resource] URL: http://www.iss.europa.eu/uploads/media/cp076 .pdf.
[11] Popp Robert; Poindexter John. Countering Terrorism through Information and Privacy Protection Technologies. IEEE Security & Privacy. 2006, Volume 4, Issue 6, pp. 18-27.
[12] Ryan J. J. C. H. Information security tools and practices: what works? IEEE Transactions on Computers, 2004, Volume: 53, Issue: 8, pp. 1060 – 1063.
[13] Schjolberg S., Ghernaouti-Hélie S. A Global Treaty on Cybersecurity and Cybercrime, Second edition, 2011. [Electronic resource] URL: http://www.cybercrimelaw.net/documents/.
[14] Talib Shuhaili; Clarke Nathan L.; Furnell Steven M. An Analysis of Information Security Awareness within Home and Work Environments. 2010 International Conference on Availability, Reliability and Security, 2010, pp.196-203.
[15] The promotion of a culture of security for information systems and networks in OECD countries. [Electronic resource] URL: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2005)1/FINAL&docLanguage=En.
[16] AlHogail Areej, Mirza Abdulrahman. Information security culture: A definition and a literature review. 2014 World Congress on Computer Applications and Information Systems (WCCAIS), 2014, IEEE, pp.1-7.
[17] Ngo L. Zhou, W. Warren, M. Understanding transition towards organizational culture change. Proceedings of the 3rd Australian Information Security Management Conference, Perth Australia, 2005.

[18] Ruighaver, A.B. & Maynard, S. Organizational Security Culture: More Than Just an End-User Phenomenon. Proceedings of the 21st IFIP TC-11 International Information Security Conference (IFIP/SEC 2006). May 22, 2006, Karlstad, Sweden, pp. 425-430.
[19] Ruighaver, A.B., Maynard, S. & S. Chang (2006) Organizational Security Culture: Extending the End-User Perspective. Computers & Security, Volume 26, Issue 1, February 2007, pp. 56-62.
[20] Sunthoshan Govender; Elmarie Kritzinger; Marianne Loock. The influence of national culture on information security culture.2016 IST-Africa Week Conference, Year: 2016, pp. 1–9.
[21] Cybersecurity policy making at a turning point. Analysing a new generation of national cybersecurity strategies for the Internet Economy. [Electronic resource] URL: http://www.oecd.org/officialdocuments/.
[22] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. [Electronic resource] URL: http://www.ftc.gov/bcp/conline/edcams/infosecurity/popups/OECD_guidelines.pdf.
[23] Summary of responses to the survey on the implementation of the OECD guidelines for the security of information systems and networks: towards a culture of security. [Electronic resource] URL: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2003)8/FINAL&docLanguage=En.
[24] Commission of the European Communities “Commission Decision of 22 April 2005 establishing the European Research Advisory” Official Journal of the European Union. Board (2005/516/EC), 2005.
[25] Commission of the European Communities. “Critical Infrastructure Protection in the Fight against Terrorism” (COM(2004)702). 2004, [Electronic resource] European Commission. URL: http://europa.eu.int/comm/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf.
[26] Commission of the European Communities. “Green Paper on a European Programme for Critical Infrastructure Protection” (COM(2005) 576), 2005. [Electronic resource] European Commission. URL: http://www.libertysecurity.org/IMG/pdf/EC_-_Green_Paper_on_CI_-_17.11.2005.pdf.
[27] Communication: A strategy for a Secure Information Society. 31.05.2006. [Electronic resource] European Commission. URL: http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=2766 .
[28] Council Resolution of 22 March 2007 on a Strategy for a Secure Information Society in Europe. Council of the European Union, Official Journal of the European Union. (C68 /01), 2007. [Electronic resource] EUR-Lex. Access to European Union law. URL: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/c_068/c_06820070324en00010004.pdf.
[29] European Commission Information Society. “Availability and Robustness of Electronic Communication Infrastructures (ARECI) Study”. [Electronic resource] URL: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/areci_study/index_en.htm .
[30] European Commission Justice and Home Affairs. “Freedom, Security and Justice; Protect Infrastructures”. [Electronic resource] URL: http://ec.europa.eu/justice_home/fsj/terrorism/protection/fsj_terrorism_protection_infrastruct_en.htm.
[31] Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection. European Commission Justice and Home Affairs. 2006. [Electronic resource] URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006PC0787 :EN:NOT.
[32] Network and Information Security: Commission seeks to improve network and information security in Europe. 31.05.2006. [Electronic resource] European Commission. URL: http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=2679.
[33] EISAS Roadmap, ENISA, 2011. [Electronic resource] The European Union Agency for Network and Information Security (ENISA). URL: https://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap.
[34] FISHA project, [Electronic resource] The Framework for Information Sharing and Alerting (FISHA). URL: http://fisha-project.eu /.
[35] Dandurand Luc, Serrano Oscar . Towards improved cyber security information sharing. 2013 5th International Conference on Cyber Conflict (CYCON 2013), IEEE Conference Publications, 2013, pp.1-16.
[36] Desourdis Robert I., Contestabile John M. Information sharing for situational understanding and command coordination in emergency management and disaster response. 2011 IEEE International Conference on Technologies for Homeland Security(HST), 2011, pp. 26 – 32.
[37] Do Hoang Giang, Ng Wee Keong . Privacy-preserving approach for sharing and processing intrusion alert data. 2015 IEEE Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP). 2015, pp.1-6.
[38] Feledi Danie, Fenz Stefan. Challenges of Web-Based Information Security Knowledge Sharing. 2012 Seventh International Conference on Availability, Reliability and Security, 2012, pp.514-521.
[39] Holgado Pilar; López de Vergara Jorge E.; Villagrá Víctor A.; Sanz Iván; Amaya Antonio. Sharing information about security alerts using semantic web technologies. 2010 International Conference on Network and Service Management, 2010, pp. 270-273.
[40] Ivanc Blaž ; Blažič Borka Jerman. Information Security Aspects of the Public Safety Data Interoperability Network. 2016 European Intelligence and Security Informatics Conference (EISIC), 2016, pp. 88–91.
[41] Kokkonen Tero ; Hautamäki Jari, Siltanen Jarmo, Hämäläinen Timo. Model for sharing the information of

cyber security situation awareness between organizations. 23rd International Conference on Telecommunications (ICT), 2016, IEEE Conference Publications, pp. 1-5.
[42] EISAS Basic Toolset report, ENISA, 2011. [Electronic resource] The European Union Agency for Network and Information Security (ENISA). URL: https://www.enisa.europa.eu/publications/eisas-basic-toolset.
[43] Bishop M. Education in information security. IEEE Concurrency.2000, Volume 8, Issue 4, pp.4-8.
[44] Chia, P. Maynard, S., and Ruighaver, A.B. 'Exploring Organisational Security Culture' Sixth Pacific Asia Conference on Information Systems, Tokyo, Japan, 2-3 September 2002.
[45] Chia, P. Maynard, S., and Ruighaver, A.B. 'Understanding Organisational Security Culture' in Information Systems: The Challenges of Theory and Practice, Hunter, M. G. and Dhanda, K. K. (eds), Information Institute, Las Vegas, USA, 2003, pp. 335 - 365.
[46] Dojkovski, S., Lichtenstein, S and Warren, M. Information Security Culture in Small and Medium Sized Enterprises: A Socio-Cultural Framework, Proceedings of 6th Australian Information Warfare & Security Conference, School of Information Systems, Deakin University, Geelong, Australia, 2005.
[47] Dojkovski, S., Lichtenstein, S. and Warren, M. Challenges in Fostering an Information Security Culture in Australian Small and Medium Sized Enterprises, Proceedings of the 5th European Conference on Information Warfare and Security, Academic Conference Limited, United Kingdom, 2006.
[48] EISAS Deployment Feasibility Study ENISA, 2013. [Electronic resource] The European Union Agency for Network and Information Security (ENISA). URL: http://www.enisa.europa.eu/publications/eisas-deployment-feasibility-study.
[49] Network and Information Security: Commission seeks to improve network and information security in Europe. 31.05.2006. [Электронный ресурс] European Commission. URL: http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=2679.
[50] EISAS Large-Scale Pilot, Collaborative Awareness Raising for EU Citizens & SMEs ENISA, 2012. [Electronic resource] The European Union Agency for Network and Information Security (ENISA). URL: https://www.enisa.europa.eu/.../eisas-large-scale-pilot.

Поступила в редакцию – 10 декабря 2017 г. Окончательный вариант – 05 февраля 2018 г.
Received – December 10, 2017. The final version – February 05, 2018.