A.A. Maluk, O.Y. Polyanskaya
National Research Nuclear University MEPHI, 115409, Moscow, Kashirskoe sh., 31,
e-mail: AAMalyuk@mephi.ru, ORCID iD is 0000-0002-5746-1508;
e-mail: OYPolyanskaya@mephi.ru, ORCID iD is 0000-0001-9867-3278

Foreign experience of the formation of information security culture in society

Keywords: information culture, information security awareness, information security culture, culture of cybersecurity

In the context of ever increasing information dependence of all spheres of activity of the company reliability and dependability of information and communication technologies (ICT), quality of information, which is used by members of the information society, saving secrets is of paramount importance. Users must trust all information services they use. Otherwise, the consequences for society and each individual can be simply disastrous. Thus, one of the main problems of the development of the information society is to ensure the information security of the individual, society and state.

In order to successfully resist the flow of threats and challenges, each member of the information society must have a certain minimum knowledge, culture and appropriate information to be prepared for an active struggle for the purity of the various types of ICT cyber-hawks, cybercriminals, cyber-terrorists and just cyber-bullies. At the same time, as shown by statistics and sociological research, while rapidly increasing the level of the use of global information and communication networks the level of information literacy of users and their information culture is extremely low. Only about 10 percent of people are more or less aware of the dangers they face while working on the Internet, or they (unwillingly) is subjected to its correspondents.

Thus, today the key issue of the Information Society becomes the formation of information culture of users and, above all, raising their awareness in this area. Analysis of approaches and expertise to solve this problem (especially overseas) is the subject of this article. The conceptual and substantive plans for the material of the article is based on a UN General Assembly resolution that approved in December 2002 the principles of formation of global culture of cybersecurity.

А.А. Малюк, О.Ю. Полянская
Национальный исследовательский ядерный университет «МИФИ», 115409, г. Москва, Каширское ш., 31, e-mail: AAMalyuk@mephi.ru, ORCID iD is 0000-0002-5746-1508; e-mail: OYPolyanskaya@mephi.ru, ORCID iD is 0000-0001-9867-3278

ЗАРУБЕЖНЫЙ ОПЫТ ФОРМИРОВАНИЯ В ОБЩЕСТВЕ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ[1]

Ключевые слова: информационная культура, осведомленность по вопросам информационной безопасности, культура информационной безопасности, культура кибербезопасности

В условиях все возрастающей информационной зависимости всех сфер деятельности общества надежность и безотказность информационно-коммуникационных технологий (ИКТ), качество информации, которой пользуются члены информационного общества, сохранение секретов приобретают первостепенное значение. Пользователи должны доверять всем используемым ими информационным сервисам. Иначе последствия для общества и каждого отдельного человека могут быть просто катастрофическими. Таким образом, одной из самых главных проблем развития информационного общества становится обеспечение информационной безопасности личности, общества и государства.

Чтобы успешно противостоять потоку вызовов и угроз, каждому члену информационного общества необходимо обладать определенным минимумом знаний, соответствующей информационной культурой и быть готовым к активной борьбе за чистоту ИКТ от раз-

[1] Работа выполнена при финансовой поддержке РГНФ. Проект № 15-03-00248: Проведение научных исследований по направлению «Формирование в обществе культуры информационной безопасности».

личного рода кибермошенников, киберпреступников, кибертеррористов и просто киберхулиганов. В то же время, как показывают статистика и социологические исследования, при быстро возрастающем уровне использования глобальных информационно-коммуникационных сетей уровень информационной грамотности пользователей и их информационной культуры оказывается крайне низким. Только около 10 процентов пользователей в той или иной степени осведомлены об опасностях, которым они подвергаются, работая в Интернете, или которым они (не желая того) подвергают своих корреспондентов.

Таким образом, сегодня ключевой проблемой развития информационного общества становится формирование информационной культуры пользователей и, прежде всего, повышения уровня их осведомленности в этой сфере. Анализ подходов и опыта решения этой проблемы (в первую очередь зарубежных) составляет предмет настоящей статьи. В концептуальном и содержательном планах изложение материала статьи основано на резолюции Генеральной Ассамблеи ООН, утвердившей в декабре 2002 года принципы формирования глобальной культуры кибербезопасности.

Введение

Существенное изменение характера и типа технологий, образующих информационную и коммуникационную инфраструктуру в современном мире, повсеместное распространение Интернета, высокопроизводительных персональных компьютеров, беспроводных и мобильных устройств привели к появлению новых возможностей ведения бизнеса и предоставления государственных услуг гражданам и предприятиям, возникновению новых способов общения людей между собой и обмена информацией друг с другом. Все это естественно сопровождается значительным расширением разнообразия пересылаемой информации, ростом ее объема и степени конфиденциальности.

Пользователи информационных систем, сетей и связанных с ними услуг все в большей мере зависят от их надежности и защищенности. В этих условиях уровень обеспечения информационной безопасности личности, общества и государства в значительной степени определяется общим уровнем информационной культуры и, особенно, культуры информационной безопасности. Для того чтобы стимулировать формирование и совершенствование культуры информационной безопасности, необходимы не только грамотное руководство и планирование в этой сфере, но и широкое участие заинтересованных сторон и осознание ими необходимости обеспечения безопасности. Участвующие стороны, в соответствии со своими ролями и функциями, должны быть осведомлены о рисках в сфере информационной безопасности и способах защиты, должны брать на себя ответственность и принимать меры, направленные на повышение безопасности информационных систем и сетей.

Отправной точкой для формирования культуры информационной безопасности в развитых странах стали рекомендации Организации экономического сотрудничества и развития (ОЭСР) «*OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*» («Руководящие принципы по безопасности информационных систем и сетей: «На пути к культуре безопасности») [1], принятые в 2002 году. Эти рекомендации легли в основу Резолюции Генеральной Ассамблеи ООН «Создание глобальной культуры кибербезопасности», принятой в декабре 2002 года.

История вопроса

Итак, можно считать, что рекомендации ОЭСР явились фактически первым из известных документов, посвященных проблеме формирования в обществе культуры информационной безопасности. В этом документе первыми по значимости принципами упоминались:

1) *осведомленность*: участники должны быть осведомлены о необходимости обеспечить безопасность информационных систем и сетей и о том, что может быть сделано для повышения безопасности; и

2) *ответственность*: все участники несут ответственность за безопасность информационных систем и сетей.

Руководящие принципы ОЭСР подчеркнули важность глобальной ответственности за предоставление гражданам информации, связанной с вопросами информационной безопасности, а также констатировали, что достаточная осведомленность и образованность в этой сфере предотвращают некомпетентное или неправильное поведение пользователей. Это, в свою очередь, укрепляет доверие к инфраструктуре и сервисам ИКТ, механизмам обеспечения безопасности и управления. Указанные руководящие принципы создали основу для формирования в обществе культуры информационной безопасности.

В 2003 и 2004 годах ОЭСР провела опрос, чтобы выяснить, какие шаги предприняли правительства стран-участниц организации по реализации «Руководящих принципов ОЭСР для безопасности информационных систем и сетей: «На пути к культуре безопасности». Опрос показал, что почти все правительства стран-участниц ОЭСР завершили разработку своих национальных стратегий формирования культуры безопасности информационных систем и сетей [2]. Большинство стран, принявших участие в опросе, сообщили о мерах, направленных на повышение осведомленности граждан по вопросам информационной безопасности, в том числе об инициативах, адресованных конкретным группам населения: широкой общественности, предприятиям малого и среднего бизнеса, молодым пользователям и новичкам в освоении информационных технологий [3].

Страны мира различаются по уровню развития ИКТ, и хотя все они сталкиваются с похожими проблемами информационной безопасности, подходы к решению этих проблем зачастую зависят от культуры страны, контекстов и национальных правовых рамок. При формировании культуры информационной безопасности одна из главных задач – правильно определить, в чем заключаются глобальные и международные проблемы и каковы локальные специфические потребности такой культуры [5]. Международные стандарты могут способствовать выявлению лишь глобальных и общих основных вопросов, связанных с культурой информационной безопасности. Каждая национальная культура при этом будет иметь свои особенности, обусловленные локальными и временными факторами. Любая глобальная стратегия развития культуры информационной безопасности должна быть адаптирована к локальным потребностям каждой страны. Поэтому особый интерес представляет изучение и обобщение опыта развитых стран по формированию у граждан культуры информационной безопасности. Прежде всего, интерес представляют способы ведения информационно-просветительской и пропагандистской работы с населением, меры, направленные на повышение уровня осведомленности в области безопасного использования интернет-сервисов, подходы к организации консультативной помощи и общественной работы по прекращению оборота противоправного контента.

Реализация основных принципов

Многие страны активно выступают с инициативами по повышению уровня культуры информационной безопасности граждан и, прежде всего, их осведомленности о существующих угрозах и мерах защиты. Эти инициативы включают в себя как организацию публичных мероприятий, так и распространение информационных материалов. Тематика общественных мероприятий варьируется от общих вопросов информационной безопасности до более конкретных проблем, таких как управление рисками безопасности, использование электронных удостоверений личности, электронных карт медицинского страхования, электронных подписей и сертификатов открытых ключей. Информационно-просветительские кампании охватывают разные целевые группы от широкой общественности до специалистов, работающих в государственных организациях и частных компани-

ях. Правительства развитых стран повышают уровень культуры информационной безопасности государственных служащих, предлагая большой выбор семинаров и конференций, и даже иногда привлекают к этим мероприятиям представителей частного сектора и граждан.

Наряду с такими средствами формирования культуры информационной безопасности как подготовка и распространение бесплатных информационных материалов, рекомендаций и руководств, правительства многих стран все больше внимания уделяют разработке лучших практик по конкретным техническим и эксплуатационным вопросам таким, как онлайн-аутентификация, цифровые подписи, беспроводная связь, управление рисками и реагирование на инциденты информационной безопасности. Все чаще информация по безопасности распространяется посредством телевидения, в социальных сетях и через рассылку *SMS*-сообщений. Анализ результатов опроса стран-участниц ОЭСР по поводу реализации «Руководящих принципов ОЭСР для безопасности информационных систем и сетей» [3] позволил выявить наиболее распространенные меры по формированию у граждан культуры информационной безопасности и способы ведения информационно-просветительской и пропагандистской работы с населением (см. табл. 1).

Таблица 1. Меры по повышению осведомленности граждан по вопросам информационной безопасности.

Меры по повышению осведомленности граждан	Страны
Создание национальной системы кибероповещения пользователей	США
Внедрение системы электронных государственных услуг	Австрия, Нидерланды
Организация сайта «Центр раннего оповещения о вирусах и компьютерной безопасности» для пользователей Интернета	Испания
Реализация национальной программы компьютерной грамотности	Чехия
Проведение рабочих совещаний, семинаров, обучения, конференций по информационной безопасности и публикация соответствующих трудов и исследований	Австралия, Чехия, Франция, ФРГ, Венгрия, Япония, Корея, Мексика, Нидерланды, Португалия, США
Привлечение средств массовой информации к информационно-пропагандистской деятельности в области информационной безопасности	Финляндия, Корея, Нидерланды, США
Организация информационно-просветительских кампаний	Дания, ФРГ, Испания
Организация сайтов и порталов по вопросам информационной безопасности	Австралия, Финляндия, Франция, ФРГ, Япония, Корея, Нидерланды, Португалия, Испания, Швеция, Великобритания, США
Организация сайтов, ориентированных на пользователей без опыта работы с ИКТ и Интернетом	ФРГ, Японии, Нидерланды, Швеция, Великобритания, США
Организация сайтов и информационных ресурсов для повышения осведомленности граждан в области информационной безопасности	Канада, США, Норвегия
Выпуск информационных бюллетеней, издание публика-	Австралия, Дания, Финлян-

Меры по повышению осведомленности граждан	Страны
ций, руководств, справочников и брошюр по информационной безопасности	дия, Франция, ФРГ, Нидерланды, Швеция, США
Подготовка и распространение бесплатных информационных материалов, правил, рекомендаций, методологии, передовых практик и руководств по информационной безопасности	Венгрия, ФРГ, Дания, США, Финляндия, Франция
Участие в ассоциациях, федерациях, обществах по профилю информационной безопасности	ФРГ
Создание комитета для повышения осведомленности по вопросам информационной безопасности	Италия
Создание «горячих» линий для консультаций по вопросам информационной безопасности	США
Организация конкурсов по безопасности информационных систем и сетей для широкой общественности	Корея
Организация серии встреч в разных городах (роуд-шоу) по вопросам информационной безопасности	Австралия
Инициатива «доверия и безопасности» в рамках реализации программы электронного правительства	Австрия
Организация национальных обучающих туров для повышения осведомленности граждан в области информационной безопасности	Корея
Интерактивный онлайновый дискуссионный форум для общения граждан и других участников с правительственными органами	Финляндия
Распространение электронных карт медицинского страхования	Австрия, ФРГ
Внедрение услуг онлайн-банкинга с мобильными электронными подписями	Австрия
Онлайновые лекции по информационной безопасности	Япония
Онлайновые технические консультации для пользователей Интернета	Япония

Наиболее масштабный проект реализован в США, там создана Национальная система кибероповещения (*National Cyber Awareness System – NACS*) [9], которая предоставляет своевременную и полезную информацию пользователям, помогая им поддерживать безопасность своих компьютерных систем. Система оповещения ориентирована на пользователей с разными уровнями компьютерной подготовки, от профессионалов с техническим образованием до пользователей домашних компьютеров. Кроме того, Федеральная торговая комиссия США, для того чтобы способствовать просвещению потребителей и расширить распространение печатных изданий и веб-публикаций на темы, связанные с информационной безопасностью, в течение многих лет сотрудничает с такими коалициями, как Альянс против мошенничества в телемаркетинге и электронной коммерции (*Alliance Against Fraud in Telemarketing and Electronic Commerce*), Национальный альянс кибербезопасности (*National Cyber Security Alliance*), Рабочая группа по борьбе с фишингом (*Anti-Phishing Working Group*) и другие.

В Чешской Республике Министерством информатики была запущена национальная программа компьютерной грамотности, направленная на обучение начинающих пользователей основным навыкам работы на компьютере и в Интернете, повышение осведомленности по вопросам информационной безопасности. Этот проект реализовывался на прин-

ципах государственного и частного партнерства, в 145 городах Чехии было организовано 240 центров обучения. Наибольший интерес к программе проявили граждане в возрасте от 40 до 60 лет.

Некоторые страны организуют конкретные периодические мероприятия (день или неделю информационной безопасности) с целью повышения осведомленности граждан о существующих угрозах информационной безопасности и практических мерах защиты от них (Финляндия, Корея, США). Так, например, в Финляндии в рамках национальной стратегии информационной безопасности была создана широкая коалиция различных государственных органов, частных компаний и других организаций, для учреждения Национального дня информационной безопасности, ежегодного мероприятия, проводимого в феврале. В Корее проводится ежегодная «Неделя информационной безопасности» (в третью неделю июня), а также учреждена «Премия по информационной безопасности» для поощрения тех компаний и университетов, которые поддерживают хороший уровень информационной безопасности и способствуют повышению общего уровня информационной безопасности в частном секторе. Кроме того, в Корее проводился национальный обучающий тур, направленный на повышение осведомленности граждан в области информационной безопасности, а также был организован ряд семинаров для распространения самой последней информации по ключевым вопросам политики и технологии информационной безопасности.

Австрия поощряет своих граждан осваивать новые, более безопасные технологии, предлагая им использовать электронные карты медицинского страхования (*the eCard*), услуги электронного правительства и вводя новую форму онлайн-банкинга с «мобильными» электронными подписями. В Австрии был введен знак качества электронного правительства (*E-Government Quality Mark*), присуждаемый тем решениям электронного правительства, которые удовлетворяют определенным критериям качества, в том числе безопасности.

Управление по делам потребителей в промышленности Канады организовало шлюз *Consumer Information Gateway* (*consumerinformation.ca*) для доступа граждан ко всей информации и услугам, предоставляемым как правительством Канады, так и неправительственными организациями. Этот информационный ресурс для потребителей базируется на партнерстве 400 федеральных министерств и ведомств, областных и территориальных министерств и неправительственных организаций. Он предлагает широкий спектр публикаций по кибербезопасности, по защите финансовой конфиденциальности в киберпространстве, защите от спама, от кражи личных данных, по безопасности электронных покупок.

Финляндия организовала онлайновый дискуссионный форум для общения граждан и других участников с правительственными органами (*www.otakantaa.fi*). Министерство финансов Финляндии использовало этот форум для интерактивных дискуссий с гражданами по вопросам информационной безопасности. В обсуждении этих вопросов приняли активное участие члены Правительственного Совета по управлению информационной безопасностью (*VAHTI*).

В Германии были реализованы инициативы со стороны федерального правительства, включающие просветительские кампании и услуги, предлагаемые Федеральным ведомством по информационной безопасности для домашних хозяйств и населения в целом, а также финансируемый правительством проект по техническим и нормативным основам электронного голосования.

В Японии для граждан страны был организован сайт по информационной безопасности *MIC Information Security Site for the People* [7]. Кроме того, японское Министерство экономики, торговли и промышленности (*METI*), а также Национальное агентство полиции (*NPA*) в сотрудничестве с некоммерческими организациями (НКО) проводят для обычных ИТ-пользователей по всей стране регулярные семинары по противодействию компьютерным вирусам и несанкционированному доступу. Наконец, портал безопасности Национального агентства полиции *@police* [8] предоставляет онлайновые лекции по без-

опасности и технические консультации для пользователей Интернета.

В Нидерландах с 2007 года развернута система предоставления электронных государственных услуг *DigiD* по уникальному сервисному номеру гражданина (*Burger Service Nummer – BSN*). Регистрационные данные (логин и пароль) позволяют пользователю получить доступ к растущему числу государственных услуг в Интернете. По закону с 6 января 2014 года *BSN* должны получать также и нерезиденты, например, голландские пенсионеры за рубежом или физические лица из ЕС, временно выполняющие сезонную работу в Нидерландах. В 2015 году к системе государственных услуг Нидерландов были подключены министерства и ведомства, налоговые органы, органы юстиции, прокуратура, банк социального страхования, муниципалитеты, открытый Университет Нидерландов, региональные социальные службы, пенсионные фонды, полиция, окружные органы, сайты провинций и т.д.

Норвегия для повышения уровня осведомленности граждан в области информационной безопасности запустила сайт *nettvett.no*. Его целевыми группами являются, прежде всего, потребители и индивидуальные предприниматели. На сайте размещаются советы по защите приватности в Интернете (своих учетных записей, личных данных, фотографий), правила поведения в чатах и социальных сетях, рекомендации по онлайн-банкингу, совершению безопасных покупок в интернет-магазинах, выбору надежных паролей, безопасному обмену данными, советы по защите от вирусов, червей, троянских программ, шпионского ПО, кибератак.

В Испании Генеральный директорат по развитию информационного общества поддержал просветительские кампании по вопросам информационной безопасности, организованные Ассоциацией пользователей Интернета в сотрудничестве с промышленностью. Через традиционные СМИ был представлен сайт для широкой общественности с инструкциями, рекомендациями и свободно распространяемыми программными средствами по информационной безопасности. Кроме того, компанией *Red.es* был организован сайт «Центр раннего оповещения о вирусах и компьютерной безопасности» (*alerta-antivirus.red.es*), который бесплатно предоставляет пользователям Интернета подробную информацию о вирусах, актуализированных оповещениях и резервный каталог предыдущих предупреждений о вирусах. На сайте также доступна подписка на бесплатные периодические отчеты и информационный бюллетень с предупреждениями о вирусах. Сайт предлагает общую информацию о компьютерной безопасности, об уязвимостях, а также обновления для безопасности программного обеспечения, дискуссионные форумы и консультационные услуги экспертов.

В Дании проводились просветительские кампании, адресованные гражданам страны, и распространялись информационные материалы по проблемам информационной безопасности.

Некоторые развитые страны разработали ряд мер повышения осведомленности по вопросам информационной безопасности для такой целевой аудитории как малый и средний бизнес (см. табл. 2).

Таблица 2. Меры по повышению осведомленности представителей малого и среднего бизнеса по вопросам информационной безопасности.

Меры по повышению осведомленности представителей малого и среднего бизнеса	Страны
Распространение информационных печатных материалов, публикация руководств по безопасности для предприятий малого и среднего бизнеса	Нидерланды, Швеция
Организация семинаров по стране по проблемам информационной безопасности	Япония

Организация сайтов и порталов по безопасности в Интернете, адресованных предприятиям малого и среднего бизнеса,	Австралия, Швеция, Великобритания
Реализация проекта Центра ресурсов по компьютерной безопасности для малого бизнеса	США
Реализация программы электронных навыков в бизнесе и администрировании (проект организации Initiative D21)	ФРГ

Так, например, Австралия организовала портал по вопросам безопасности и выпустила специальный пакет информационных ресурсов для предприятий малого и среднего бизнеса. В Швеции был создан сайт о безопасности в Интернете, адресованный предприятиям малого и среднего бизнеса, и распространялись печатные информационные материалы для этой категории пользователей. Правительство Великобритании в партнерстве с промышленностью организовало ресурс *UK Online for Business* («Великобритания онлайн для бизнеса»). Центр ресурсов по компьютерной безопасности США разработал специальный проект для малого бизнеса. В Японии Агентство по продвижению информационных технологий *Information Technology Promotion Agency* (*IPA*) и Японский центр координации групп экстренного реагирования на компьютерные инциденты *Japan Computer Emergency Response Team Coordination Centre* (*JPCERT/CC*) регулярно проводит семинары по всей стране, посвященные способам защиты от компьютерных вирусов и несанкционированного доступа, адресованные руководителям информационных систем.

Многие успешные информационно-просветительские и пропагандистские кампании по формированию культуры информационной безопасности в странах ОЭСР были реализованы, прежде всего, в сфере образования и адресовались детям, молодежи, родителям школьников и пожилым людям (см. табл. 3). Большинство инициатив направлено на просвещение детей и студентов либо через учителей, преподавателей и родителей, либо путем прямого распространения информационных материалов. Информационно-просветительские инициативы было поручено организовать различным агентствам или министерствам, например: Совету по ИТ-безопасности (Дания), Министерству финансов (Финляндия), Федеральному бюро по информационной безопасности (ФРГ), Национальному агентству полиции (Япония), Министерству торговли и промышленности и Министерству юстиции (Норвегия), Министерству науки и технологий (Испания), Федеральной торговой комиссии (*FTC*, США) и Национальному институту стандартов и технологий (*NIST*, США).

Таблица 3. Меры по формированию культуры информационной безопасности в системе образования

Целевая аудитория	Меры в системе образования	Страны
Дети, школьники	Проведение конкурсов лозунгов и плакатов для учащихся школ по безопасности информационных систем и сетей	Корея
	Выпуск журнала комиксов о безопасном использовании Интернета	Нидерланды
	Организация интернет-викторин по вопросам безопасного поведения в интернете	США
	Распространение комиксов об интернет-зависимости, учебников, компьютерных игр по информационной безопасности для детей	Корея
	Организация сайта для маленьких детей, только начинающих пользоваться Интерне-	Австралия

Целевая аудитория	Меры в системе образования	Страны
Дети, школьники	том, и создание обучающей системы *Netty'sWorld*, позволяющей во время онлайновой игры получать сообщения, касающиеся информационной безопасности	
	Поддержка общенационального центра компетенции для преподавания и обучения школьников безопасному поведению в интернете	ФРГ
	Организация портала по безопасному использованию Интернета для детей	Япония
	Обеспечение развивающими учебниками и играми	Корея
	Размещение на специальном сайте советов детям и викторины по правилам сетевой этики	Нидерланды
	Создание сайта для детей *www.4Kids.org* с функцией еженедельной газеты	США
	Организация конкретных периодических мероприятий (дня или недели информационной безопасности) для продвижения информационной безопасности в образовательных учреждениях	Финляндия, Корея, США
	Организация сдачи экзаменов и выдачи дипломов за знание безопасного использования Интернета	Нидерланды
Молодежь, студенты	Организация сайтов по безопасности в Интернете, адресованных молодежи	ФРГ
	Предоставление детям и молодежи безопасного и контролируемого педагогами доступа к Интернету в рамках проекта «*Jugendans Netz*» («Молодежь в Сети»)	ФРГ
	Проведение в университетских городках информационно-просветительских кампаний по обучению правилам защиты своих личных данных и безопасности в Интернете	США
	Предоставление стипендий студентам, обучающимся информационной безопасности	США, ФРГ
	Финансовая поддержка тех, кто пишет диссертации по тематике информационной безопасности в научных учреждениях	ФРГ
	Спонсирование программы подготовки специалистов по информационной безопасности, защищающих критически важную информационную инфраструктуру правительства	США
	Введение карт с электронной подписью для студентов и учащихся	Австрия
	Учреждение премии по информационной безопасности для университетов и компаний	Корея
Молодежь, студенты	Разработка и внедрение в университетах политик безопасности информационных систем	Канада

Целевая аудитория	Меры в системе образования	Страны
	и сетей	
	Создание государственного центра обучения безопасности информационных систем (*CFSSI*)	Франция
	Создание центра реагирования на компьютерные инциденты *CERT* для образовательных учреждений	Нидерланды Финляндия
Учителя, преподаватели	Обеспечение учебными материалами и презентациями по безопасности в Интернете	Австралия, Финляндия, ФРГ, США
	Создание общенационального центра компетенции для преподавания и обучения «*SchulenansNetz*» («Школы в Сети»), способствующего распространению новых медиасредств в школах	ФРГ
	Обеспечение методическими материалами для обучения детей онлайновой безопасности	Финляндия
	Включение вопросов информационной безопасности в образовательные программы	Испания
Родители детей и школьников	Организация веб-сайтов для детей и их родителей по безопасному использованию Интернета и мобильных технологий	США, Япония, Австралия, Испания, Норвегия
	Обеспечение родителей курсами, информирующими о рисках информационной безопасности	Нидерланды, США
	Обеспечение родителей методическими материалами для обучения детей онлайновой безопасности	Финляндия
Пожилые люди	Организация сайтов-клубов или центров обучения компьютерным навыкам и использованию Интернета для пожилых людей	Норвегия
	Реализация программы онлайновой компетентности граждан старше 50 лет	ФРГ
	Организация портала, публикующего образовательные материалы по информационной безопасности и советы пожилым людям	Испания
	Проведение ежегодных дней открытых дверей в библиотеках и центрах общения для людей среднего возраста и пожилых по вопросам участия в информационном обществе	Норвегия

Многие страны участвуют в инициативе *dotSafe* [6] европейской организации *Europe.Schoolnet*, международного партнерства более чем 26 министерств образования европейских стран, развивающих обучение онлайн-безопасности для школ, учителей и, а также тесно сотрудничают с Европейской сетью центров безопасного Интернета (*www.saferinternet.org*). Направлениями деятельности этих центров в области онлайн-безопасности являются ведение информационно-просветительской работы и повышение осведомленности в области безопасного использования цифровых сервисов, содействие

развитию позитивного контента и его популяризация, общественная работа по прекращению оборота противоправного контента, консультативная помощь. Основное внимание уделяется наиболее незащищенным категориям пользователей – детям и подросткам, а также тем, кто их защищает – родителям, работникам сферы образования и воспитания, экспертам, тем, кто принимает решения, социальным работникам.

Для сравнения кратко отметим, что в России в 2008 году для работы в рассматриваемых направлениях был создан проект «Центр безопасного Интернета», позднее названный Центром безопасности в информационном обществе «НеДопусти!». На сайте российского центра *www.nedopusti.ru* можно найти информационно-просветительские статьи и видеоматериалы, тематические новости и мнения экспертов, а также воспользоваться «Горячей линией по противоправному контенту» и консультационной «Линией помощи».

Взаимодействие с участниками информационного общества

Партнерство и взаимодействие с другими участниками (бизнесом, промышленностью, ассоциациями потребителей, образовательными организациями) в сфере повышения осведомленности в области безопасного использования интернета характерно для многих стран.

Между 2009 и 2011 годами несколько стран-членов ОЭСР инициировали разработку стратегий нового поколения – стратегий кибербезопасности. В 2012 году в документе Рабочей группы по информационной безопасности и конфиденциальности ОЭСР «*Cybersecurity policy making at a turning point. Analysing a new generation of national cybersecurity strategies for the Internet Economy*» [4] приводились результаты опроса 10 стран-участниц ОЭСР по поводу результатов реализации национальных стратегий кибербезопасности, призванных способствовать экономическому и социальному процветанию стран и защищать киберпространство от угроз при сохранении открытости Интернета в качестве платформы для инноваций и новых источников роста.

Опрос показал, что для современных стратегий кибербезопасности важными попрежнему остаются такие направления, как повышение уровня информированности и образования по вопросам информационной безопасности в обществе. Просветительские инициативы, как правило, направлены на все население в целом, включая такую целевую группу, как дети (Австралия, Испания, Великобритания), а также на предприятия, государственные органы (особенно на лиц, принимающих решения) и критически важные инфраструктуры. Повышение уровня образования населения в сфере информационной безопасности достигается, например, за счет обучения «кибергигиене» в школах (Нидерланды), использования социальных СМИ (Великобритания), проведения совместных просветительских кампаний с интернет-провайдерами с помощью создания сервиса поддержки в области информационной безопасности (Япония) [4]. Великобритания поддерживает развитие рыночных дифференциаторов: сертифицированных этикеток безопасности для продуктов и услуг, а также промышленных стандартов и рекомендаций. Нидерланды создали учебный центр по кибербезопасности. Австралия поддерживает концепцию ответственного цифрового гражданства, основанного на грамотности и осведомленности в сфере цифровых технологий, позволяющих пользоваться преимуществами Интернета и эффективно снижать киберриски.

В настоящее время нехватка специалистов по кибербезопасности рассматривается правительствами многих стран как ключевая политическая задача. США, например, сравнивают эту ситуацию с усилиями по модернизации науки и математического образования в 1950-е годы. Великобритания стремится поощрять развитие сообщества "этичных хакеров". Эти меры включают, например, создание программы сертифицированного обучения специалистов (Нидерланды, Великобритания), поддержку инициативы *Cyber Security Challenge* (*cybersecuritychallenge.org.uk*). *Cyber Security Challenge* – это британский некоммерческий проект по проведению ежегодных онлайновых конкурсов по ИТ-

безопасности с целью привлечения талантливых людей в эту индустрию. Проект помогает профессионалам любого возраста развивать карьеру в области кибербезопасности.

Выводы (современное состояние)

В течение трех десятилетий ОЭСР играет важную роль в формировании культуры информационной безопасности в обществе, в продвижении политики и инструментов для инноваций и доверия в цифровой экономике. В 2012 году Рабочей группой ОЭСР по безопасности и конфиденциальности в цифровой экономике (*Working Party on Security and Privacy in the Digital Economy – SPDE*) была начата работа по пересмотру «Руководящих принципов по безопасности информационных систем и сетей: «На пути к культуре безопасности». 25 июня 2015 года пересмотренные рекомендации были обсуждены и одобрены Комитетом по политике цифровой экономики ОЭСР. В новом документе первыми по значимости общими принципами безопасности упоминаются [10]:

1. Осведомленность, навыки и расширение прав и возможностей.

Все заинтересованные стороны должны понимать риск цифровой безопасности и как управлять им. Они должны знать, что риск цифровой безопасности может повлиять на достижение их экономических и социальных целей и что их управление риском цифровой безопасности может повлиять на других. Они должны обладать образованием и навыками, необходимыми для понимания этого риска, чтобы помогать управлять им, а также для оценивания потенциального воздействия своих решений по управлению рисками цифровой безопасности на свою деятельность и цифровую среду в целом.

2. Ответственность.

Все заинтересованные стороны должны взять на себя ответственность за управление риском цифровой безопасности. Они должны действовать ответственно на основе их ролей, контекста и их способности действовать, нести ответственность за управление риском цифровой безопасности и за принятие во внимание потенциального воздействия их решений на других.

Они должны осознавать, что необходимо принять определенный уровень риска цифровой безопасности для достижения экономических и социальных целей.

3. Права человека и основные ценности

Все заинтересованные стороны должны управлять риском цифровой безопасности прозрачно и в соответствии с правами человека и фундаментальными ценностями.

Управление риском цифровой безопасности должно быть реализовано таким образом, чтобы оно согласовалось с правами человека и фундаментальными ценностями, признанными демократическими обществами, включая свободу выражения мнений, свободное распространение информации, конфиденциальность информации и коммуникации, неприкосновенность частной жизни и персональных данных, открытый и справедливый суд. Управление риском цифровой безопасности должно основываться на этичном поведении, которое уважает и признает законные интересы других лиц и общества в целом. Организации должны иметь общую политику прозрачности их практики и процедур управления риском цифровой безопасности.

Эти рекомендации Совета ОЭСР были приняты 17 сентября 2015 года, они стали новыми ориентирами в деятельности развитых стран по совершенствованию культуры информационной безопасности и кибербезопасности в современном обществе.

СПИСОК ЛИТЕРАТУРЫ:

1. OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. (http://www.ftc.gov/bcp/conline/edcams/infosecurity/popups/OECD_guidelines.pdf)
2. The promotion of a culture of security for information systems and networks in OECD countries. (http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2005)1/FINAL&docLanguage=En)
3. 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.
(http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2003)8/FINAL&docLanguage=En)
4. Cybersecurity policy making at a turning point. Analysing a new generation of national cybersecurity strategies for the Internet Economy. (http://www.oecd.org/officialdocuments/)
5. Schjolberg S., Ghernaouti-Hélie S. A Global Treaty on Cybersecurity and Cybercrime, Second edition, 2011. (http://www.cybercrimelaw.net/documents/)
6. The dotSAFE project. (http://www.dotsafe.eun.org)
7. MIC Information Security Site for the People. (http://www.soumu.go.jp/joho_tsusin/security/index.htm)
8. Internet Security Portal Site @police. (https://www.npa.go.jp/cyberpolice/)
9. National Cyber Awareness System. (https://www.us-cert.gov/ncas)
10. Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris. DOI. (http://dx.doi.org/10.1787/9789264245471-en)

REFERENCES:

1. OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.
(http://www.ftc.gov/bcp/conline/edcams/infosecurity/popups/OECD_guidelines.pdf)
2. The promotion of a culture of security for information systems and networks in OECD countries. (http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2005)1/FINAL&docLanguage=En)
3. 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.
(http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2003)8/FINAL&docLanguage=En)
4. Cybersecurity policy making at a turning point. Analysing a new generation of national cybersecurity strategies for the Internet Economy. (http://www.oecd.org/officialdocuments/)
5. Schjolberg S., Ghernaouti-Hélie S. A Global Treaty on Cybersecurity and Cybercrime, Second edition, 2011. (http://www.cybercrimelaw.net/documents/)
6.The dotSAFE project. (http://www.dotsafe.eun.org)
7. MIC Information Security Site for the People. (http://www.soumu.go.jp/joho_tsusin/security/index.htm)
8. Internet Security Portal Site @police. (https://www.npa.go.jp/cyberpolice/)
9. National Cyber Awareness System. (https://www.us-cert.gov/ncas)
10. Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris. DOI. (http://dx.doi.org/10.1787/9789264245471-en)