Анатолий А. Малюк, Зоя П. Малюк
Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
e-mail: AAMalyuk@mephi.ru, http://orcid.org/0000-0002-5746-1508

АКТУАЛЬНЫЕ ВОПРОСЫ СОЗДАНИЯ СИСТЕМЫ МАССОВОГО ОБУЧЕНИЯ КУЛЬТУРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

DOI: http://dx.doi.org/10.26583/bit.2021.4.01

Аннотация. Интенсивно развивающиеся в России процессы формирования информационного общества ставят на повестку дня проблему повышения уровня информационной культуры общества и, прежде всего, такой ее части, как культура информационной безопасности. Практика показывает, что общество нуждается в организации эффективного «всеобуча» в области защиты информации в современных технических средствах ее сбора, обработки, передачи и хранения. В Доктрине информационной безопасности Российской Федерации, утвержденной Президентом страны в декабре 2016 г., неоднократно отмечается важность проблемы формирования культуры личной информационной безопасности граждан, являющихся, в частности, активными пользователями Интернета и других современных инфокоммуникационных систем. В связи с этим в статье рассматриваются актуальные вопросы формирования системы непрерывного обучения членов информационного общества в области основ обеспечения информационной безопасности, начиная с самых ранних лет (со школы или даже с детского сада). В статье излагается политика формирования культуры информационной безопасности, формулируются подходы к организации системы массового обучения, предлагаются конкретные меры по их реализации. Как пример работы в этом направлении описывается инновационный образовательный кластер, созданный совместным решением Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации и Департамента образования и науки г. Москвы.

Ключевые слова: информационное общество, информационная безопасность, информационная культура, непрерывное образование, массовое обучение, формирование культуры личной информационной безопасности.

Для цитирования: МАЛЮК, Анатолий А.; МАЛЮК, Зоя П. АКТУАЛЬНЫЕ ВОПРОСЫ СОЗДАНИЯ СИСТЕМЫ МАССОВОГО ОБУЧЕНИЯ КУЛЬТУРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Безопасность информационных технологий, [S.l.], т. 28, № 4, с. 6–21, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1373. DOI: http://dx.doi.org/10.26583/bit.2021.4.01.

Anatoly A. Malyuk, Zoya P. Malyuk
National Nuclear Research University MEPHI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia,
e-mail: AAMalyuk@mephi.ru, http://orcid.org/0000-0002-5746-1508

Topical issues of creating a mass education system for information security culture

DOI: http://dx.doi.org/10.26583/bit.2021.4.01

Abstract. The rapidly developing processes of the information society formation in Russia put on the agenda the problem of improving the information culture of society and, above all, such a part of it as the culture of information security. The practice demonstrates a need in organising an effective "universal education" in the field of information protection for modern technical means of its collection, processing, transmission and storage. The Information Security Doctrine of the Russian Federation, approved by the President of the country in December 2016, repeatedly notes the importance of the problem of forming a culture of personal information security of citizens who are, in particular, active users of the Internet and other modern information and communication systems. In this regard, the article deals with topical issues of the formation of a system of continuous training of members of the information society in the field of the basics of information security, starting from the earliest years (from school or even from

kindergarten). The paper describes the policy of forming a culture of information security, formulates approaches to the organisation of mass education systems, and suggests specific measures for their implementation. As an example of the progress in this direction, an innovative educational cluster created by a joint decision of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation and the Department of Education and Science of Moscow is described.
Keywords: information society, information security, information culture, continuing education, mass education, formation of a culture of personal information security.
For citation: MALYUK, Anatoly A.; MALYUK, Zoya P. Topical issues of creating a mass education system for information security culture. IT Security (Russia), [S.l.], v. 28, no. 4, p. 6–21. 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1373. DOI: http://dx.doi.org/10.26583/bit.2021.4.01.

Введение

Формирование культуры информационной безопасности как одна из наиболее актуальных проблем развития информационного общества в Российской Федерации в последнее время начинает, наконец, привлекать к себе внимание и занимать соответствующее место среди общественных интересов. Следует отметить, что в Доктрине информационной безопасности Российской Федерации[1], принятой в 2016 г., неоднократно отмечается низкий уровень культуры личной информационной безопасности, а также недостатки в организации массового обучения граждан основам информационной культуры и грамотности в условиях бурного развития современных информационно-коммуникационных технологий (ИКТ). В подтверждение этого приведем обобщенные данные различных статистических источников и результаты социологических исследований, которые показывают, что сегодня в России число пользователей глобальной сети Интернет приближается к 100 млн чел. В то же время доля имеющих хотя бы минимальное представление об опасностях, которым они подвергают себя и других, не превышает 10% [1].

Отметим, что на протяжении всей истории человечества информационные процессы изначально играли важнейшую роль, являясь основой механизмов поведения и общения, сохранения идентичности и развития личности, управления производственной и экономической деятельностью. Все это неминуемо приводит к постоянному развитию и совершенствованию механизмов накопления, запоминания, передачи и обработки информации и при постоянном увеличении ее объемов. Последний фактор приводит, в конечном счете, к возникновению своего рода информационных барьеров, выход из которых общество находит, каждый раз совершенствуя информационные процессы.

Естественно, что в этих условиях наблюдается постоянно растущая зависимость, как отдельных личностей, так и общества в целом, а также его основных институтов от качества используемой информации. В результате такой усиливающейся информационной взаимосвязанности общество в целом и отдельные индивидуумы подвергаются все более многочисленным и разнообразным угрозам, которые создают новые проблемы в плане обеспечения безопасности. Когда важные данные не удается эффективно защитить, под угрозой находится личная безопасность людей, безопасность бизнеса и, что еще важнее, национальная безопасность государств.

Таким образом, проблема защиты информации становится личным, деловым и национальным приоритетом и в той или иной мере затрагивает каждого члена общества. Практика показывает, что эффективность политики обеспечения информационной

[1]Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
URL: https//publication.parvo.gov.ru/Document/View/0001201612060002 (дата обращения: 15.09.2021).

безопасности на 80% зависит от мер организационно-правового и гуманитарного характера. При этом действия государственных или правоохранительных органов, направленные на обеспечение безопасности, должны осознанно поддерживаться всем обществом. Отсюда следует, что предприятия, организации, индивидуальные владельцы и пользователи продуктов ИТ-индустрии должны знать о факторах, угрожающих информационной безопасности, и возможных превентивных действиях, должны сознавать свою ответственность и принимать меры для повышения безопасности информационных технологий. Таким образом, в современном обществе должна быть сформирована культура информационной безопасности, которая является составной частью общей информационной культуры.

1. Основы политики формирования культуры информационной безопасности

Под культурой информационной безопасности принято понимать знания и навыки граждан и организаций, позволяющие им безопасно использовать информационные и телекоммуникационные технологии в своей деятельности и принимать меры, направленные на выявление и нейтрализацию угроз, способных нанести им тот или иной ущерб. При этом важнейшей составляющей культуры информационной безопасности являются правила, нормы и стандарты безопасного использования информационных и телекоммуникационных технологий, в том числе этические нормы [2–5].

Становление нового уровня культуры информационной безопасности должно рассматриваться во взаимосвязи с формированием современных общественных и производственных отношений и происходящими в обществе социальными изменениями. В связи с этим основными факторами, влияющими на уровень культуры информационной безопасности современного общества, можно считать:

- состояние системы образования, которая, в конечном счете, определяет общий уровень интеллектуального развития людей, их материальные и духовные потребности;
- состояние информационной инфраструктуры, от которой зависит возможность безопасно получать, передавать и использовать необходимую информацию, оперативно осуществлять те или иные информационные коммуникации;
- уровень демократизации общества, который обеспечивает правовые гарантии доступа людей к необходимой им информации;
- экономическую состоятельность страны, гарантирующую возможность получения ее гражданами необходимого образования, а также приобретения и использования ими современных продуктов ИТ-индустрии.

Таким образом, как видим, уровень культуры информационной безопасности непосредственно зависит от важнейших характеристик общественного развития и может служить интегральным показателем состояния общества [6].

Основные методы и подходы к решению проблем формирования культуры информационной безопасности должны увязывать воспитательные, просветительские, образовательные и производственные аспекты деятельности личности, общества и государства в целях реализации следующих взаимодополняющих элементов информационной политики[23]:

[2]Резолюция Генеральной Ассамблеи ООН A/RES/57/239 «Создание глобальной культуры кибербезопасности».
URL:http://daccessdds.un.org/doc/UNDOC/GEN/N02/738/25/PDF/N0273825.pdf?OpenElement (дата обращения: 15.09.2021).

- повышение осведомленности членов глобального информационного общества о необходимости обеспечения безопасности информационных систем и сетей и о том, что они могут для этого сделать;
- повышение ответственности членов глобального информационного общества за безопасность информационных систем и сетей сообразно с ролью каждого из них;
- совершенствование реагирования членов информационного общества, которые должны принимать своевременные и совместные меры по предупреждению инцидентов, затрагивающих безопасность, их обнаружению и принятию необходимых мер по их нейтрализации;
- решение этических проблем повсеместного использования информационных систем и сетей в современном обществе, связанных с учетом законных интересов других сторон [7, 8];
- совершенствование демократических основ информационного общества, в котором безопасность должна обеспечиваться так, чтобы это соответствовало ценностям общества, включая свободу обмена мыслями и идеями, свободный доступ к информации, конфиденциальность информации и коммуникации, надлежащую защиту информации личного характера, открытость и гласность;
- совершенствование подходов и методов оценки риска, направленных на выявление угроз и факторов уязвимости, анализ ключевых внутренних и внешних факторов, сказывающихся на безопасности, выбор надлежащих инструментов контроля, позволяющих регулировать риск потенциального ущерба информационным системам и сетям с учетом характера и значимости защищаемой информации;
- совершенствование организации проектирования и внедрения средств обеспечения безопасности;
- совершенствование управления обеспечением безопасности, предусматривающее применение комплексного подхода и опирающееся на динамичную оценку риска, охватывающую все уровни деятельности членов общества и все аспекты их операций;
- своевременная переоценка вопросов безопасности информационных систем и сетей и внесение надлежащих изменений в политику, практику, меры и процедуры обеспечения безопасности, учитывающие появление новых и изменение прежних угроз и факторов уязвимости.

Таким образом, основной целью политики в области формирования культуры информационной безопасности является укрепление государственных гарантий реализации конституционных прав и свобод в информационной сфере [9, 10] и привлечение потенциала участников информационно-телекоммуникационных взаимодействий для повышения уровня защищенности этих взаимодействий от угроз информационной безопасности.

2. Всеобуч в области культуры информационной безопасности

Очевидно, что одним из наиболее важных механизмов повышения компетентности в области информационных технологий и формирования культуры информационной безопасности является массовое обучение людей. Цель такого обучения – научить ценить безопасность, ответственно использовать компьютерные технологии, своевременно

[3]Указ Президента Российской Федерации от 05.12.2016 №646 «Об утверждении Доктрины информационной безопасности Российской Федерации». URL: https://publication.pravo.gov.ru/Document/View/0001201612060002 (дата обращения: 15.09.2021).

реагировать на инциденты, связанные с нарушением безопасности, владеть способами восстанавливать компьютерные системы и информацию после таких инцидентов, грамотно обращаться с доказательствами, которые могут потребоваться во время судебного расследования компьютерных преступлений, а также тому, как и кому сообщать об инцидентах, связанных с нарушением информационной безопасности. Практика показывает, что обучение основам информационной безопасности и преподавание этики использования компьютерных технологий больше способствуют укреплению безопасности, чем какие-либо другие меры. Без преподавания нравственности и этики, особенно молодым людям, по всей видимости, не будут преодолены проблемы компьютерной и сетевой безопасности.

Таким образом, не вызывает никаких сомнений высокая актуальность проблемы формирования информационной культуры у подрастающего поколения [11]. Обучение в данном случае может быть профессиональным и массовым. Профессиональное обучение ориентировано на целевую аудиторию (студентов средних специальных и высших учебных заведений, слушателей курсов повышения квалификации или центров переподготовки и сертификации специалистов в области информационной безопасности). Проблемы развития такого обучения являются предметом особого разговора и выходят за рамки данной статьи. Отметим здесь только, что обучение морали, этике и ответственному использованию информации и информационных технологий, интегрированное в гуманитарные и естественнонаучные дисциплины призвано выполнять уникальную функцию подготовки студентов к жизни в информационном обществе [12].

И еще одно замечание относительно профессионального обучения. Современная жизнь требует от всех специалистов-профессионалов постоянного повышения квалификации, непрерывного обновления знаний, освоения новых видов деятельности. В идеале повышение образовательного уровня человека должно продолжаться в течение всей жизни. В связи с этим сегодня особенно актуальна идея «образования в течение всей жизни» или, как принято говорить, непрерывного образования [13].

Реализация этой идеи связана с дополнительным обучением на тренингах, семинарах или курсах повышения квалификации с последующим получением соответствующего сертификата. Повышением квалификации специалистов в области информационной безопасности сегодня занимаются не только профильные вузы, но и учебные центры дополнительного образования (как правило, негосударственные), созданные компаниями и организациями, активно работающими на рынке средств и услуг, связанных с защитой информации.

Возвращаемся к основной теме нашей статьи – массовому обучению. Его цель состоит в том, чтобы вовлечь в процесс обучения как можно больше людей и добиться максимального эффекта при ограниченных ресурсах. Сегодня главным здесь, несомненно, будет использование возможностей глобальной сети Интернет и создание специальных онлайн-курсов. Второе – это совершенствование общеобразовательной подготовки в рамках средней общеобразовательной школы. Оба эти направления заслуживают отдельного рассмотрения, и будут рассмотрены подробно ниже. Здесь же отметим некоторые другие подходы, которые способствуют достижению конечной цели массового обучения.

Первое, что можно использовать – это организация местных, региональных и национальных мероприятий и благотворительных акций. Аналогичный подход к решению серьезных социальных проблем (таких, как распространение СПИД, COVID-19 и других угрожающих жизни заболеваний) позволил, как свидетельствует практика, быстро и достаточно эффективно обеспечить повышение осведомленности населения. Таких же

результатов можно ожидать и от акций, посвященных проблемам обеспечения информационной безопасности и возможным превентивным мерам в этой области.

Другое направление – это создание специальных информационных центров. Наблюдающийся в последнее время взрывной рост преступлений, совершаемых с использованием Интернета, побудил государственные органы ряда стран создать центры, информирующие о киберпреступлениях. Эти центры занимаются сбором информации о компьютерных инцидентах в киберпространстве и доведением ее до широкой общественности. Роль центров в повышении осведомленности граждан о проблемах информационной безопасности достаточно велика. Они функционируют в качестве первого пункта контактов в тех случаях, когда происходит или предполагается, что произошел, компьютерный инцидент. Центры также консультируют тех, кто хочет больше узнать о мерах, которые используют в целях выявления и предотвращения сетевых вторжений, а также о способах восстановления систем и данных после успешных кибератак.

Помимо рассмотренных методов повышения информированности и массового обучения есть и другие, которые можно использовать, хотя они и являются менее эффективными. Эти методы попадают в так называемую категорию активистской деятельности, то есть общественно-политического движения, пропагандирующего активное вмешательство граждан в решение острых социальных и политических проблем. К этим методам относится пропаганда и создание «горячих линий». Информационно-пропагандистские группы могут работать с общественностью, корпорациями и правительством для того, чтобы повысить уровень осознания обществом проблем современного компьютеризированного мира и повлиять на формирование культуры информационной безопасности. Стратегия вовлечения в кампании большого числа граждан, несомненно, приносит плоды в виде массового осознания угроз личной, корпоративной и национальной безопасности, которое ведет к усилению общественного давления на законодателей и государственные органы, вынуждая их должным образом защищать интересы граждан и общества.

«Горячие линии» позволяют широкой общественности брать на себя инициативу в наблюдении и уведомлении о компьютерных инцидентах. В большинстве случаев стратегия заключается в организации приема сообщений по каналам такой линии от свидетелей инцидентов компьютерной безопасности. Ответственными за прием сообщений и принятие соответствующих мер являются в этом случае правоохранительные органы и поставщики услуг Интернета.

В целом задача формирования современной культуры информационной безопасности требует использования возможностей всех звеньев системы непрерывного образования для повышения осведомленности всех членов общества о проблемах безопасности информационных систем и сетей, осознания каждым человеком своей роли и ответственности, обучения людей этике в сфере информационных технологий, целенаправленной деятельности государственных органов, больших общественных усилий по нескольким фронтам: в сфере законодательства, нормативного регулирования, а также активной деятельности граждан.

3. Онлайн-курсы для реализации системы массового обучения культуре информационной безопасности

Сосредоточимся теперь на проблеме образования. Очевидно, что решение вопросов формирования в обществе культуры информационной безопасности помимо учета, рассмотренного выше, в образовательных программах всех уровней подготовки, начиная

со школы, требует также создания и развития системы массового обучения. Такое обучение можно реализовать, наверное, только с использованием современных дистанционных технологий. Рассмотрим, как это обстоит сегодня.

В настоящее время в Интернете можно найти достаточно большое число онлайн-курсов, которые в той или иной мере могли бы быть использованы в реализации системы массового обучения культуре информационной безопасности (ИБ). Чтобы оценить реальную возможность их массового использования, проанализируем их содержание, имея в виду концепцию формирования культуры ИБ, предложенную в рассмотренной выше резолюции Генеральной Ассамблеи ООН.

С этих позиций перечень ресурсов, которые уже сегодня можно было бы использовать при обучении в целях формирования культуры ИБ, может быть представлен следующими работами [14–22].

Анализ приведенных ресурсов приводит к следующим выводам:

1. К принятой ООН концепции формирования глобальной культуры кибербезопасности наиболее близко подходят три курса, разработанные в НИУ ВШЭ [14–16]. При этом содержательно курсы [14] и [16] очень похожи. Курс [15] сосредоточен, в основном, на организационно-правовых методах защиты информации. Все эти курсы используют один и тот же сценарий видео-лекции и подготовлены одним и тем же автором, старшим преподавателем МИЭМ, А.В. Сорокиным. Общий недостаток курсов НИУ ВШЭ – не рассмотрены гуманитарные аспекты, а также проблемы собственно формирования культуры информационной безопасности, что, кстати, отмечено в качестве основных проблем в Доктрине информационной безопасности Российской Федерации (2016 г.).

2. Определенный интерес представляют также курсы, разработанные в Нью-Йоркском и Вашингтонском университетах [17–21]. Однако в содержательном плане они отличаются от принятого в России подхода, начиная с различия терминов, например, «информационная безопасность» и «кибербезопасность». Это постоянный терминологический спор, во многом связанный с политическими вопросами.

3. По отдельным технологическим подходам к решению конкретных проблем обеспечения информационной безопасности определенный интерес представляет курс, разработанный Массачусетским технологическим институтом [22]. Отдельные элементы этого курса вполне могут быть использованы при создании некоторого базового курса по культуре ИБ. Однако использовать его как основу реализации такого курса нельзя.

4. В сети Интернет присутствует достаточно много онлайн-курсов, разработанных компанией «Microsoft». Однако следует отметить, что все они ориентированы на отдельные продукты данной компании, поэтому могут быть рекомендованы как примеры, иллюстрирующие решение вопросов обеспечения безопасности конкретных информационных объектов.

Таким образом, очевидно, что на повестке дня главным актуальным вопросом создания системы массового обучения в области формирования культуры информационной безопасности оказывается проблема разработки базового онлайн-курса. Дадим ему условное название «Информационная безопасность и цифровая экономика».

Ниже как один из возможных подходов приведена рабочая программа данного онлайн-курса, которая представляет, на наш взгляд, основные его элементы и может явиться основой для разработки конкретных курсов, имеющих различную целевую аудиторию.

РАБОЧАЯ ПРОГРАММА БАЗОВОГО ОНЛАЙН КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЦИФРОВАЯ ЭКОНОМИКА»

ЦЕЛИ ОСВОЕНИЯ КУРСА. Целями освоения курса являются усвоение обучающимися основных положений Доктрины информационной безопасности Российской Федерации, Стратегии развития информационного общества в России, получение представления о предметной области комплекса наук о безопасности, качественных и количественных методах описания жизненно важных интересов личности, общества и государства, множества угроз безопасности, получение необходимых предварительных знаний общих вопросов обеспечения безопасности информации в автоматизированных системах, ознакомление с основными понятиями и терминологией в области защиты данных и программ в компьютерах и компьютерных сетях, основными проблемами обеспечения безопасности информации, методами их решения, современными научными направлениями, связанными с решением этих проблем, воспитание в гражданах правового сознания и морально-этических качеств, отвечающих требованиям этики в сфере информационных технологий.

КОМПЕТЕНЦИИ, ПРИОБРЕТАЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ КУРСА. В результате освоения курса каждый обучающийся должен:

Знать:

- сущность и понятие информации, информационной безопасности и характеристики составляющих их элементов;
- место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России;
- источники и классификацию угроз информационной безопасности;
- основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;
- способы и средства защиты информации от утечки по техническим каналам;
- основы организационного и правового обеспечения информационной безопасности.

Уметь:

- классифицировать защищаемую информацию по видам тайны и степени конфиденциальности;
- классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;
- анализировать и оценивать угрозы информационной безопасности объекта;
- применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
- оценивать информационные риски в автоматизированной системе.

Владеть:

- терминологией в области информационной безопасности;
- криптографической терминологией;
- методами оценки информационных рисков.

СОДЕРЖАНИЕ КУРСА.

Курс «Информационная безопасность и цифровая экономика» включает следующие разделы:

Раздел 1

Цифровая экономика как этап информатизации, при котором данные становятся новым ключевым элементом экономики, влияющим на добавленную стоимость. История цифровой экономики. Современный ареал распространения цифровой экономики. Программа развития цифровой экономики в России. Цели и основные направления Программы. Совершенствование нормативного регулирования. Кадровое сопровождение Программы. Формирование исследовательских компетенций и технологических заделов. Развитие информационной инфраструктуры. Защищенность и безопасность – необходимые условия реализации всех разделов Программы развития цифровой экономики.

Раздел 2

Новые перспективные направления развития современных информационно-коммуникационных технологий. «Умный» город. Цифровые здравоохранение и образование. Интернет вещей. Распределенное хранение данных (блокчейн). Технологии больших данных. Сети пятого поколения.

Раздел 3

Обеспечение информационной безопасности как важнейший элемент развития цифровой экономики. Терминология в области информационной безопасности. Основные защищаемые свойства информации – конфиденциальность, целостность, доступность. Подходы к обеспечению информационной безопасности. Уязвимость информации. Угрозы информационной безопасности (нарушение конфиденциальности, целостности и доступности данных). Понятие компьютерной атаки. Основные типы атак. Компьютерные хакеры. Модель нарушителя. Политика безопасности. Основные методы обеспечения информационной безопасности. Субъекты и объекты информационной безопасности. Механизмы обеспечения информационной безопасности (аутентификация, авторизация, аудит). Применение криптографических методов защиты. Симметричные и несимметричные алгоритмы шифрования. Хэширование. Защита информации от несанкционированного доступа (НСД). Дискреционная и мандатная модели разграничения доступа. Модель Белла и Ла Падула. Модель Биба. Ролевая модель доступа. Модель безопасности информационных потоков. Искусственный интеллект в системах безопасности.

Раздел 4

Обеспечение безопасности новых технологий. Оценка безопасности Интернета вещей. Безопасность технологии «блокчейн». Безопасность сетей 5*G*. Безопасность больших данных. Выводы по материалам курса и задачи пользователей в области обеспечения информационной безопасности современных ИКТ.

Как пример практической реализации такого онлайн-курса можно рассматривать авторский курс «Глобальная культура кибербезопасности», размещенный в рамках Национального форума «Информационная безопасность России в условиях глобального информационного общества» («Инфофорум») [23].

4. Создание инновационного образовательного кластера для подготовки будущих специалистов ИТ-отрасли и формирования в обществе культуры информационной безопасности

Остановимся на реализации политики в области формирования в обществе культуры информационной безопасности на уровне средней общеобразовательной школы. В качестве примера рассмотрим запущенный в марте 2014 г. Министерством связи и массовых коммуникаций Российской Федерации (ныне Министерство цифрового развития, связи и массовых коммуникаций) совместно с Департаментом образования г. Москвы совместный проект по подготовке школьников в сфере ИТ. Цели данного проекта:

- создание в Москве системы подготовки мотивированных учащихся, имеющих необходимый уровень компетенций для дальнейшего образования и работы в области ИТ;
- уменьшение «кадрового голода» в технологической сфере экономики;
- выработка организационно-нормативных механизмов реализации образовательных проектов на базе образовательных организаций совместно с ведущими ИТ-компаниями;
- развитие содержания образования в области информатики и ИТ, поддерживающего необходимый уровень информационной культуры современного общества.

Проект, как считают организаторы, позволил к настоящему времени увеличить количество школьников, выбирающих инженерно-технические или естественнонаучные специальности при поступлении в вузы, и привел к росту числа выпускников, желающих работать в ИТ-отрасли.

Задачи современного образования предполагают становление в образовательной системе механизмов общественно-государственного управления. Эти механизмы являются неотъемлемой составляющей развития гражданского общества в нашей стране.

С помощью этих механизмов в 2007 г. была создана некоммерческая организация – Общероссийское общественное движение творческих педагогов «Исследователь» (ООДИ). В настоящее время движение имеет свои отделения в 60 субъектах Российской Федерации.

Московское городское отделение ООДИ было образовано в сентябре 2010 г. Возглавила его Духанина Л.Н., президент частного образовательного холдинга (школа, детский сад) «Наследник», заведующая кафедрой педагогики и методики естественнонаучного образования НИЯУ МИФИ, заместитель председателя комиссии по развитию науки и образования Общественной Палаты Российской Федерации, член Исполкома Общероссийского Народного Фронта, депутат Государственной Думы Российской Федерации VII созыва.

В составе Московского ООДИ более 60 общеобразовательных учреждений столицы: лицеи, гимназии, центры образования с лицейскими и гимназическими классами, школы с углубленным изучением ряда предметов. Большинство из них – это учреждения, выступающие, как правило, локомотивами образовательных инициатив и инноваций в системе столичного образования, выстраивающие учебно-воспитательный процесс в рамках единой лицейско-гимназической традиции: определенная направленность, выход на профильные учреждения, специфика среды, численность учащихся и т.д.

Главное направление деятельности Московского ООДИ – это информационные технологии, информационная безопасность, информационная культура.

Универсальным алгоритмом познания и предпрофессиональных навыков (основы профильного обучения) выступает проектно-исследовательская деятельность учащихся, ключевая образовательная технология, позволяющая реализовать новое содержание образования в современной школе.

Исследовательская работа школьников сегодня включена в учебные программы многих образовательных учреждений г. Москвы. Опыт работы лучших из них показывает, что для решения поставленных задач оптимальным является включение учащихся в исследовательскую работу не только на уроках, в рамках учебных занятий, но и, в большей степени, в системе дополнительного образования, которое, как правило, поддерживает и развивает профиль.

В целях интеграции накопленного опыта в организации профильного обучения в области ИТ-технологий в апреле 2014 г. инициативная группа наиболее продвинутых общеобразовательных учреждений в союзе с тремя профильными учреждениями высшего образования договорилась о создании сетевого инновационного кластера.

Учреждения кластера имеют уникальный опыт в организации профильного обучения старшеклассников и в течение последних лет входят в списки ТОП-400, ТОП-500 и т.д. Их учащихся всегда можно видеть в числе победителей и призеров многих региональных и Всероссийских олимпиад, конкурсов, фестивалей. Все учреждения кластера имеют хорошо выстроенные отношения с вузами, связанными с реализацией профильного обучения, с проведением профориентационной работы и т.д.

Для образовательной системы понятие «кластер» можно определить как совокупность образовательных, научных, производственных и других организаций и реализуемых на их базе форм образовательной деятельности в определенной предметно-тематической области. В данном случае, это – информационные технологии, информационная безопасность, информационная культура, связанные сетевым образом.

В числе достоинств кластерной организации образования отметим:

- возможность использования всеми участниками кластера разнообразных ресурсов (кадры, материально-техническая база и др.), имеющихся у производственных предприятий, общественных организаций, вузов и т.д.;
- введение в сферу образования наиболее современного предметного и технологического содержания, только появляющихся в современной науке и производстве;
- возможность повышения преемственности образования на разных уровнях, начиная с дошкольного и заканчивая высшим;
- повышение мотивации школьников к творческой деятельности и осознанному выбору профессии – построение индивидуальных образовательных траекторий, способствующих раннему становлению профессионализма.

Последовательное освоение продвинутыми учащимися методов проектно-исследовательской деятельности поможет им на практике освоить различные методы получения, анализа, обработки, представления и защиты информации.

Сформулируем далее возможные направления дальнейшего развития деятельности образовательного кластера. Среди них выделим:

I. Организационно-методические мероприятия

- Разработка, обсуждение и утверждение на педагогических советах образовательных учреждений, заседаний кафедр вузов Положения о кластере, Плана работы на текущий и последующие учебные годы.

- Формирование рабочих групп на базе кластера, анализ состояния материально-технической базы образовательных учреждений, участвующих в реализации проекта.
- Определение и разработка программ сотрудничества участников кластера с организациями-партнерами; формирование портфеля тем для проектно-исследовательских работ старшеклассников.
- Анализ учебных программ по информатике; включение элементов учебного исследования в преподавание информатики: детский сад, 1–4 классы школы, в рамках предпрофильной подготовки в 5–8 классах, в рамках профильного обучения 9–11 классы.
- Создание банка дидактических приемов использования исследовательских методов обучения в пространстве урока по информатике, элективных курсов и специальных курсов по информационно-технологическому профилю.
- Создание электронного журнала (регистрация и т.д.).

II. Реализация системы мероприятий, поддерживающих качество образования и обеспечивающих мотивацию школьников к получению ИТ-образования, к освоению важнейших навыков и ключевых компетенций

- Участие школьников образовательных учреждений кластера в городских и Всероссийских конкурсах, конференциях, фестивалях науки, олимпиадах и т.д.
- Разработка Программы привлечения к работе с подростками, связывающих свое будущее с ИТ-отраслью, известных специалистов в области современных информационных технологий для:

а) чтения научно-популярных лекций по новым приоритетным направлениям ИТ;
б) ведения элективных, специальных курсов, факультативов, кружков;
в) руководства проектно-исследовательскими работами старшеклассников в области ИТ-технологий; консультирование и помощь в работе школьных научных обществ;
г) организации экскурсий на предприятия, фирмы, компании;
д) привлечения старшеклассников образовательных учреждений кластера к участию в научных сессиях вузов с возможными публикациями в сборниках научных трудов;
е) организации и проведения летней практики для 10-классников на базе лабораторий и кафедр вузов-партнеров, и, в первую очередь, фирм, компаний, учреждений, организаций, участвующих в кластере.

- Обязательное участие школьников образовательных учреждений кластера в Днях открытых дверей вузов, сотрудничающих с участниками в рамках кластера.
- Организация летних городских (профильных) лагерей, цель которых создание научно-образовательного пространства для развития познавательного интереса и выбора подростком собственного образовательного маршрута в информационно-технологической сфере.
- Проведение ежегодной итоговой конференции-выставки исследовательских работ учащихся образовательных учреждений-участников кластера (совместно с фирмами-партнерами) – как итог работы за год.
- Подготовка и проведение совместно с журналом «Дети в информационном пространстве» ежегодного конкурса (со временем выйти на проведение «своей» ИТ-Олимпиады на базе одного из вузов) по информатике, информационной безопасности, информационной культуре для учащихся 8–11 классов; и отдельно – для преподавателей информатики (в форме реферативных работ).

III. Программа повышения квалификации и переподготовки преподавательского корпуса образовательных учреждений

- Проведение мастер-классов по программе взаимообучения участников проекта по категориям: учителя информатики; преподаватели физики, математики; учителя начальных классов; воспитатели детского сада; учителя гуманитарных дисциплин.
- Организация курсов по программам, например, Академии CISCO для учителей и старшеклассников.
- Прохождение курсовой подготовки учителями информатики, физики, математики на базе вузов; включение в программу повышения квалификации следующих модулей:
  - современные подходы к обучению информатике и ИКТ;
  - проектно-исследовательская деятельность в процессе изучения информатики;
  - подготовка школьников к ЕГЭ по информатике.

IV. Научно-методическое обеспечение деятельности кластера

- Подготовка и издание сборника элективных курсов, которые уже «в работе» в образовательных учреждениях кластера (они расширяют образовательные области информатики, математики, физики, способствуют будущей профессиональной мотивации старшеклассников и приобретению ими начальных навыков в области информационных технологий).
- Подготовка пакета развивающих программ для системы дополнительного образования в начальной школе: робототехника, мехатроника и т.д.

V. Популяризация профессий в области ИТ-технологий и информационной безопасности

- Подготовка презентаций (с помощью и консультациями фирм партнеров по кластеру) о наиболее интересных и перспективных профессиях ИТ-направления; издание научно-популярных брошюр, буклетов по информационной безопасности, информационной культуре; выпуск Бюллетеней о людях, добившихся успехов в области ИТ (например, разработка «Кодекса юного пользователя Интернета»).
- Организация экскурсий на фирмы, в отечественные и зарубежные ИТ-компании.
- Проведение для старшеклассников мастер-классов профессионалами из ИТ-отрасли как на базе образовательных учреждений-участников кластера, так и в своих фирмах, компаниях, организациях.
- Создание фильмов-роликов.

Заключение

Чтобы развитие информационного общества и переход в эпоху цифровой экономики прошел как можно легче и была обеспечена безопасность государственных и коммерческих учреждений, а также отдельных пользователей, необходимо реализовать защищенную инфраструктуру цифровой экономики и обеспечить ее информационную и образовательную поддержку путем формирования в обществе культуры информационной безопасности. Для решения этих проблем необходимо создание системы массового обучения граждан. Это обучение должно предусматривать усвоение этических норм информационного общества, овладение законодательной базой, регулирующей развитие информационных технологий, а также освоение механизмов защиты специфических для

цифровой экономики технологий: интернета вещей, больших данных, распределенного хранения данных и сетей пятого поколения. Основой такого массового обучения должна явиться единая образовательная среда, охватывающая все уровни образования, практически от детского сада до высших учебных заведений, и система онлайн-курсов, размещаемых в сети Интернет.

Самое серьезное внимание в настоящее время должно быть уделено общеобразовательной средней школе, закладывающей основы нравственности и информационной грамотности будущего поколения. Реальным механизмом реализации данной задачи может явиться инновационный образовательный кластер, успешная попытка создания которого осуществлена в г. Москве.

СПИСОК ЛИТЕРАТУРЫ:

1. Малюк А.А., Полянская О.Ю., Алексеева И.Ю. Комментарии к Доктрине информационной безопасности Российской Федерации. М.: Горячая линия – Телеком, 2018 – 102 с.; илл. URL: https://www.elibrary.ru/item.asp?id=35187777 (дата обращения: 28.02.2021).
2. Малюк А.А., Полянская О.Ю., Алексеева И.Ю. Этика в сфере информационных технологий. М.: Горячая линия – Телеком, 2011 – 344 с.; илл. URL: https://knigogid.ru/books/289941-as-nature-made-him-the-boy-who-was-raised-as-a-girl/toread (дата обращения: 28.02.2021).
3. Малюк Анатолий А.; Полянская Ольга Ю. Опыт реализации пилотного проекта европейской системы оповещения и обмена информацией по информационной безопасности. Безопасность информационных технологий, [S.l.]. Т. 25, № 1. С. 6–18, 2018. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2018.1.01.
4. Johnson D.G. Computer Ethics, Prentice-Hall, 3d Edition, 2001 – 240 p. URL: https://openlibrary.org/books/OL18389288M/Computer_ethics (дата обращения: 28.02.2021).
5. Marx G.T. An Ethics For The New Surveillance. The Information Society, 1998. Vol. 14, no. 3. P. 171–186. DOI: http://dx.doi.org/10.1080/019722498128809.
6. Малюк А.А. Проблемы формирования культуры информационной безопасности на пространстве ШОС // Проблемы социогуманитарного обеспечения инновационных процессов на евразийском пространстве. Коллективная монография / Под ред. В.Е. Лепского. М.: «Когито-Центр», 2014 – 201 с.: ил., табл., схем. URL: https://biblioclub.ru/index.php?page=book&id=430577&lang=ru (дата обращения: 28.02.2021).
7. Barger R. (2008). The Ethical Decision-Making Process. In Computer Ethics: A Case-based Approach. P. 70–79. Cambridge: Cambridge University Press. DOI: http://dx.doi.org/10.1017/CBO9780511804151.007.
8. Barger R. (2008). Computer Ethics and International Development. In Computer Ethics: A Case-based Approach. P. 107–139. Cambridge: Cambridge University Press. DOI: http://dx.doi.org/10.1017/CBO9780511804151.011.
9. Смирнов Анатолий И. Глобальные аспекты культуры кибербезопасности: взгляд из России. 2-я международная конференция «ИНФОФОРУМ-Болгария». URL: https://infourok.ru/globalnye-aspekty-kultury-kiberbezopasnosti-vzglyad-iz-rossii-4856020.html (дата обращения: 28.02.2021).
10. Волчинская Е. Законодательство Российской Федерации о доступе к информации: краткий обзор и анализ. МОО ВПП ЮНЕСКО «Информация для всех», 2004. URL: https://ifap.ru/projects/analytic/ea002.pdf (дата обращения: 28.02.2021).
11. Кондратенко Е.Л., Прокудин Д.Е. Обеспечение информационной безопасности как проблема отечественного школьного воспитания в условиях информационного общества. // Проблемы современного образования. 2013. № 6. С. 78–84. URL: https://elibrary.ru/item.asp?id=21183792 (дата обращения: 12.05.2021).
12. Косенко Т.С., Власюк Н.Н. Проблемы нравственного воспитания подрастающего поколения в условиях информационного общества. Философия образования, 2017, № 70, вып. 1. С. 84–90. DOI: http://dx.doi.org/10.15372/PHE20170111.
13. Павлова Е.Д. Медиаобразование как способ формирования национальной информационной культуры // Приоритетные национальные проекты: первые итоги и перспективы реализации // Отв. ред. Ю.С. Пивоваров. М.: ИНИОН РАН, 2007. С. 204–208. URL: http://inion.ru/ru/resources/starye-versii-saita/novosti-za-1998-2010-gody/arkhiv-novostei-za-2007-god/38/ (дата обращения: 28.02.2021).
14. Сорокин А.В. Методы и средства защиты информации // НИУ ВШЭ (МИЭМ им. А.Н.Тихонова). URL: https://www.coursera.org/learn/metody-i-sredstva-zashity-informacii (дата обращения: 28.02.2021).

15. Сорокин А.В. Менеджмент информационной безопасности // НИУ ВШЭ (МИЭМ им. А.Н.Тихонова). URL: https://www.coursera.org/learn/management-informacionnoi-bezopasnosti (дата обращения: 28.02.2021).
16. Сорокин А.В. Защита информации // НИУ ВШЭ (МИЭМ им. А.Н. Тихонова). URL: https://openedu.ru/course/hse/DATPRO/ (дата обращения: 28.02.2021).
17. Sanjay Goel. International Cyber Conflicts. The State University of New York. URL: https://www.coursera.org/learn/cyber-conflicts (дата обращения: 28.02.2021).
18. Barbara E. Popovsky. Finding your Cybersecurity Career Path. University of Washington. URL: https://www.edx.org/course/finding-your-cybersecurity-career-path (дата обращения: 28.02.2021).
19. Barbara E. Popovsky. Introduction to Cybersecurity. University of Washington. URL: https://www.edx.org/course/introduction-to-cybersecurity (дата обращения: 28.02.2021).
20. Barbara E. Popovsky, David Aucsmith. Find your niche in cybersecurity. University of Washington. URL: https://www.edx.org/professional-certificate/uwashingtonx-essentials-cybersecurity (дата обращения: 28.02.2021).
21. David Aucsmith. Building a Cybersecurity Toolkit. University of Washington. URL: https://www.edx.org/course/building-a-cybersecurity-toolkit (дата обращения: 28.02.2021).
22. Nickolai Zeldovich. Computer Systems Security. Massachusetts Institute of Technology. URL: https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-858-computer-systems-security-fall-2014/ (дата обращения: 28.02.2021).
23. Глобальная культура кибербезопасности // Авторский курс лекций А.А. Малюка. URL: https://infoforum.online/lektoriy/video-globalnaya-kultura-kiberbezo/ (дата обращения: 28.02.2021).

REFERENCES:

[1] Malyuk A.A.; Polyanskaya O.Y., Alekseeva I.Yu. Comments on the Information Security Doctrine of the Russian Federation. M.: Goryachaya liniya – Telekom, 2018 – 102 p.; илл. URL: https://www.elibrary.ru/item.asp?id=35187777 (accessed: 28.02.2021) (in Russian).
[2] Malyuk A.A.; Polyanskaya O.Y., Alekseeva I.Yu. Ethics in the field of information technology. M.: Goryachaya liniya – Telekom, 2018. – 344 p.; илл. URL: https://www.elibrary.ru/item.asp?id=35187777 (accessed: 28.02.2021) (in Russian).
[3] 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.]. T. 25, no. 1. P. 6–18, 2018. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2018.1.01. (in Russian).
[4] Johnson D.G. Computer Ethics, Prentice-Hall, 3d Edition, 2001 – 240 p. URL: https://openlibrary.org/books/OL18389288M/Computer_ethics (accessed: 28.02.2021).
[5] Marx G.T. An Ethics For The New Surveillance. The Information Society, 1998. Vol. 14, no. 3. P. 171–186. DOI: http://dx.doi.org/10.1080/019722498128809.
[6] Malyuk A.A. Problems of formation of information security culture in the SCO space. Problems of socio-humanitarian support of innovation processes in the Eurasian space. Collective monograph. Edited by V.E. Lepsky. M.: "Kogito-Center" 2014 - 201 p. URL: https://biblioclub.ru/index.php?page=book&id=430577&lang=ru (accessed: 28.02.2021) (in Russian).
[7] Barger R. (2008). The Ethical Decision-Making Process. In Computer Ethics: A Case-based Approach. P. 70–79. Cambridge: Cambridge University Press. DOI: http://dx.doi.org/10.1017/CBO9780511804151.007.
[8] Barger R. (2008). Computer Ethics and International Development. In Computer Ethics: A Case-based Approach. P. 107–139. Cambridge: Cambridge University Press. DOI: http://dx.doi.org/10.1017/CBO9780511804151.011.
[9] Smirnov Anatoly I. Global Aspects of Cybersecurity Culture: a View from Russia. 2nd International Conference «INFOFORUM-Bulgaria». URL: https://infourok.ru/globalnye-aspekty-kultury-kiberbezopasnosti-vzglyad-iz-rossii-4856020.html (accessed: 28.02.2021) (in Russian).
[10] Volchinskaya E. The legislation of the Russian Federation on access to information: a brief overview and analysis. Interregional Public Organization in support of the UNESCO program «Information for all», 2004. URL: https://ifap.ru/projects/analytic/ea002.pdf (accessed: 28.02.2021) (in Russian).
[11] Kondratenko E.L., Prokudin D. E. Ensuring information security as a problem of domestic school education in the conditions of the information society. Problems of modern education. 2013. No. 6. P. 78–84. URL: https://elibrary.ru/item.asp?id=21183792 (accessed: 12.05.2021) (in Russian).
[12] Kosenko T.S., Vlasyuk N.N. Problems of youths moral education in the conditions of information society. Philosophy of Education, 2017, no. 70, issue 1. P. 84–90. DOI: http://dx.doi.org/10.15372/PHE20170111 (in Russian).

[13] Pavlova E.D. Media education as a way of forming a national information culture. Priority national projects: first results and prospects of implementation. Ed. by Yu. S. Pivovarov. M.: INION RAS, 2007. P. 204–208. URL: http://inion.ru/ru/resources/starye-versii-saita/novosti-za-1998-2010-gody/arkhiv-novostei-za-2007-god/38/ (accessed: 28.02.2021) (in Russian).
[14] Sorokin A.V. Methods and means of information protection. HSE (Tikhonov MIEM). URL: https://www.coursera.org/learn/metody-i-sredstva-zashity-informacii (accessed: 28.02.2021) (in Russian).
[15] Sorokin A.V. Information Security Management. HSE (Tikhonov MIEM). URL: https://www.coursera.org/learn/management-informacionnoi-bezopasnosti (accessed: 28.02.2021) (in Russian).
[16] Sorokin A.V. Information protection. HSE (Tikhonov MIEM). URL: https://openedu.ru/course/hse/DATPRO/ (accessed: 28.02.2021) (in Russian).
[17] Sanjay Goel. International Cyber Conflicts. The State University of New York. URL: https://www.coursera.org/learn/cyber-conflicts (accessed: 28.02.2021).
[18] Barbara E. Popovsky. Finding your Cybersecurity Career Path. University of Washington. URL: https://www.edx.org/course/finding-your-cybersecurity-career-path (accessed: 28.02.2021).
[19] Barbara E. Popovsky. Introduction to Cybersecurity. University of Washington. URL: https://www.edx.org/course/introduction-to-cybersecurity (accessed: 28.02.2021).
[20] Barbara E. Popovsky, David Aucsmith. Find your niche in cybersecurity. University of Washington. URL: https://www.edx.org/professional-certificate/uwashingtonx-essentials-cybersecurity (accessed: 28.02.2021).
[21] David Aucsmith. Building a Cybersecurity Toolkit. University of Washington. URL: https://www.edx.org/course/building-a-cybersecurity-toolkit (accessed: 28.02.2021).
[22] Nickolai Zeldovich. Computer Systems Security. Massachusetts Institute of Technology. URL: https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-858-computer-systems-security-fall-2014/ (accessed: 28.02.2021).
[23] Global cybersecurity culture. Author's course of lectures by A.A. Malyuk. URL: https://infoforum.online/lektoriy/video-globalnaya-kultura-kiberbezo/ (accessed: 28.02.2021) (in Russian).

Поступила в редакцию – 28 января 2021 г. Окончательный вариант – 22 ноября 2021 г.
Received – January 28, 2021. The final version – November 22, 2021.