ЦИФРОВЫЕ ТЕХНОЛОГИИ СОВМЕСТНОЙ ПОДГОТОВКИ ПРОФЕССИОНАЛЬНЫХ КАДРОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННОЙ МЕЖДУНАРОДНОЙ ОБРАЗОВАТЕЛЬНОЙ СФЕРЕ

Соляной В.Н.
Сухотерин А.И.
ГБОУ ВО «Технологический университет», г.о. Королев, Россия

Применение технологий цифровой экономики в современном образовании при подготовке профессионалов по информационной безопасности, является одним из факторов развития и совершенствования функционирования государственных институтов, что порождает новые информационные угрозы. В настоящее время колледжи и университеты предлагают онлайн-курсы; онлайн-преподаватели новые методы изучения учебных материалов; школы регулярно интегрируют планшетные компьютеры и другие технологии в учебные аудитории. Технология меняет образование, тренды трансграничности, цифровизации и открытости субъектов информатизации делают информационный образовательный ресурс более уязвимым для негативного воздействия злоумышленников.

В работе рассмотрены возможные перспективы развития существующей подготовки кадров по информационной безопасности на базе Технологического университета (г. Королев), с учетом особенностей производственной сферы региона г. Королева и Московской области.

Ключевые слова: Информационная безопасность. система подготовки кадров, региональный центр, радиоэлектронные системы и комплексы, телекоммуникации, специалитет, бакалавриат, магистратура, университет, факультет, кафедра, техникум.

DIGITAL TECHNOLOGIES OF JOINT TRAINING OF PROFESSIONAL PERSONNEL ON INFORMATION SECURITY IN THE MODERN INTERNATIONAL EDUCATIONAL SPHERE

V.N. Solianoy
A.I. Sukhoterin
State Educational Institution of Higher Education
Moscow Region «University of technology», Korolev, Moscow region

The use of digital economy technologies in modern education in the training of information security professionals is one of the factors in the development and improvement of

the functioning of state institutions, which creates new information threats. Colleges and universities currently offer online courses; online teachers new methods of studying teaching materials; schools regularly integrate tablet computers and other technologies into classrooms. Technology changes education, trends of cross-border, digitalization and openness of informatization entities make the educational information resource more vulnerable to the negative impact of attackers.

The paper considers possible prospects for the development of existing training in information security at the Technological University (Korolev), taking into account the characteristics of the production sector of the Korolev region and the Moscow region.

Keywords: Information security, staff training system, regional center, radio-electronic system and complex, telecommunications, specialist, bachelor, magistracy, university, faculty, department, technological college.

Как показывает современная действительность существует реальная возможность избирательного информационно-технического воздействия со стороны ряда зарубежных стран на информационную инфраструктуру экономики в политических, экономических и в военных целях. При этом усиливается деятельность организаций, осуществляющих техническую разведку в отношении государственных, национальных коммерческих, научных (образовательных) организаций и предприятий оборонно-промышленного комплекса. Новые технологии, используемые иностранными компаниями, существенно понижают конкурентоспособность отечественных производителей, а информационно-психологическое воздействие позволяет существенным образом воздействовать на экономических субъектов, манипулируя спросом и предложением экономики, биржевыми котировками и т.д.

В современном образовании, науке, исследованиях, культуры и средствах массовой информации являются ключевыми областями внедрения новых цифровых достижений и сами по себе выступают в качестве важнейших факторов и способствующих дальнейшему развитию цифровых технологий. Это означает, что все граждане (субъекты информационной безопасности) могут воспользоваться огромными возможностями в различных сферах для обучения, повышения квалификации, непрерывного образования, развития и участия в экономической и социальной жизни.

Расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию экономической ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств. В эту деятельность вовлекаются религиозные, этнические, правозащитные и иные организации, а также отдельные группы граждан, при этом широко используются возможности современных информационных технологий.

В этих условиях система образования должна лучше оснащать людей навыками и знаниями, чтобы они отвечали требованиям безопасности цифровой рабочей среды и общества знаний. Она также должна повысить уровень грамотности безопасности в средствах массовой информации. Поэтому необходимо содействовать более широкому использованию безопасных цифровых средств информации в образовании на протяжении всей жизни человека. Вместе со всеми заинтересованными сторонами в области образования будет стремиться к созданию цифровой стратегии обучения [1,2,3,4,9,10], которая будет систематически использовать, расширять и внедрять возможности цифровых средств массовой информации для предоставления высококачественного образования.

Возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее. С учетом общей цифровизации человек становится полностью уязвим перед глобальными платформами, получающими полный доступ к частной информации.

Повышается сложность и увеличивается масштаб и количество скоординированных компьютерных атак на объекты критической информационной инфраструктуры. Данные риски увеличиваются с распространением Интернета вещей и облачных технологий.

Состояние информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства характеризуется стремлением отдельных государств использовать технологическое превосходство для доминирования в информационном пространстве. Существующее в настоящее время распределение между странами ресурсов, необходимых для обеспечения безопасного и устойчивого функционирования сети «Интернет», не позволяет реализовать совместное справедливое, основанное на принципах доверия управление ими. Отсутствие международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения, учитывающих специфику информационных технологий, затрудняет формирование системы международной информационной безопасности, направленной на достижение стратегической стабильности и равноправного стратегического партнерства.

Социальная адаптации населения к вызовам цифровой экономики, относящимся к непрерывному повышению уровня квалификации и развитию новых навыков в интерактивном пространстве цифровой экосистемы. В этом отношении крайне важны активная политика на рынке труда, поддержка доходов, непрерывное обучение и более гибкие образовательные системы [1,2,3,4,9,10].

Сегодня в обществе существует запрос на новых специалистов по информационной безопасности обладающих компетенциями с помощью которых будут преодолены основные барьеры на пути цифровизации экономики [1,2,3].

Первый **барьер** — неготовность предприятий заниматься развитием производства с помощью безопасных сетевых технологий. В первую очередь это связано с сознанием и уровнем квалификации менеджмента в области ИБ.

Второй **барьер** — недостаток специалистов. 90% международных компаний признают, что они испытывают дефицит «цифровых талантов», особенно в области ИБ.

Необходимых специалистов можно условно разделить на три большие группы:

Первая — специалисты, обладающие компетенциями в части описания, моделирования и оптимизации бизнес-процессов и анализа требований.

Вторая — специалисты по методам анализа данных и машинного обучения, способные применять существующие методы для решения конкретных бизнес-задач в различных отраслях.

Третья — это специалисты, способные создавать и поддерживать базовую ИТ-инфраструктуру, используемую в цифровой экономике.

Необходимо создавать специальные центры (превосходства) образования по информационной безопасности, когда существует такой вот треугольник: университет/студенты — индустрия — муниципальное участие.

Третий барьер — кибербезопасность. Нельзя недооценивать масштабы киберугрозы, особенно скорость ее распространения. Нужна следующая схема: компании создают собственные центры противодействия киберугрозам, они потом превращаются в

фьюжн-центры, а те в свою очередь смогут управлять инцидентами. Результаты работы переходят к госинститутам, после чего разрабатывается правоприменение».

Что касается информационной безопасности, то доля субъектов, использующих стандарты безопасного информационного взаимодействия государственных и общественных институтов, должна составить 75%. А доля внутреннего сетевого трафика российского сегмента Интернета, маршрутизируемая через иностранные серверы, должна составлять 5%.

Современное жесткое противостояние Российской Федерации со стороны ряда иностранных государств (в форме экономической блокады, ведения активной информационной войны и вооруженного давления) обуславливает проведения усиленных защитных мер. Ключевыми мерами в рассмотренных условиях следует рассматривать, прежде всего, проведение мероприятий по информационному противоборству (как на государственном, так и на региональных уровнях функционирования нашего государства) [1,2,3,4,9,с.359,10,с.249].

Постоянно усиливающиеся деструктивные информационные угрозы воздействуют как на промышленные (государственные и частные структуры), так и социальные (индивидуальное и коллективное сознание и подсознание) объекты (субъекты).

В связи с этим международные вопросы подготовки высококвалифицированных кадров по информационной безопасности (ИБ), в современных условиях бурного развития мирового информационного общества, рассматриваются как одно из приоритетных задач функционирования любого индустриального государства в условиях проведения против него активной информационной войны.

Данная задача актуальна и для Российской Федерации. Особенно остро подготовка профессионалов по информационной безопасности просматривается для промышленных регионов, специализирующих на оборонную сферу и разработку инновационных информационных технологий [5,с.635,6,с.640,7,с.384].

Регион Московской области является в рассматриваемом ракурсе ведущим в Российской федерации и, следовательно, поддержание информационной безопасности региона на высоком уровне рассматривается как необходимое условие обеспечения национальной безопасности нашего государства.

Данная установка и обуславливает необходимость постоянного совершенствования существующей системы информационной безопасности Московской области и, в частности, Королевского региона. Эффективное противодействие таким целенаправленным информационным угрозами (которые реализуются с использованием новейших методов и средств воздействия на человека, технику и окружающую среду) невозможно без подготовки высококвалифицированных кадров по информационной безопасности. В Московской области данную задачу выполняет всего единственное высшее образовательное учреждение – Московский государственный областной технологический университет (МГОТУ), расположенный в г. Королеве. В структуре данного образовательного учреждения и была сформирована в 2008 году кафедра Информационной безопасности по подготовки, на этапе своего становления, специалистов по защите информации (российский подход), а в настоящее время – бакалавров и магистров по информационной безопасности (международный подход.

Проведенный анализ востребованности профессионалов по данному направлению в Московской области и Королевском регионе показал необходимость дальнейшего развития существующей системы подготовки кадров по информационной безопасности в структуре Технологического университета (МГОТУ). Данное положение обуславливается усиливающейся востребованностью этих специалистов для предприятий-партнеров (работодателей) Московской области и г. Москва: РКК «Энергия»; КТРВ; ЦНИИ маш; НИИ КС; НПО «ИТ»; ЗАО «Тех ЗИ»; ООО «КЛИО»; ЦБИ; 18 ЦНИИ МО РФ; ФГУП «ЭЛЕРОН», Роскомнадзор и др.

Анализ также позволил выявить новые задачи МГОТУ в области подготовки профессионалов по информационной безопасности [1,2,3,4,9,10]:

1. Расширения и реализация дополнительных профессиональных компетенций в области информационной безопасности персонала предприятий, учреждений и организаций (руководителей и администрации, руководителей структурных подразделений и рядовых сотрудников) региона в муниципальной, производственной, образовательной и финансово- кредитной сферах;

2. Необходимость, с одной стороны, увеличения количества подготавливаемых профессионалов по информационной безопасности и, с другой стороны, целесообразность расширения видов новых специализаций, направлений и профилей у выпускников реализующих цифровые компетенции Технологического университета;

3. Возрастающую востребованность специалистов по информационной безопасности – выпускников со средним профессиональным образованием, т.е. техников по информационной безопасности (защиты информации).

С учетом выше изложенного в МГОТУ был разработан трехэтапный план развития системы подготовки профессионалов по информационной безопасности (Рис.1).

На первом этапе развития предусматривается развертывание Регионального учебно-научного (производственного) центра по проблемам информационной безопасности (РУНЦ) Московской области. Первоначально указанный РУНЦ располагается в структуре существующей кафедры Информационной безопасности МГОТУ.

Второй этап развития системы подготовки профессионалов по информационной безопасности предусматривает два под этапа.

Первоначальный под этап предполагает расширение подготовки профессионалов на существующей кафедры ИБ:

- введение по направлению подготовки бакалавр 10.03.01 «Информационная безопасность», нового профиля – «Информационно-аналитические системы финансового мониторинга» с 2016 г.;

- открытие специалитета по направлению подготовки «Радиоэлектронные системы и комплексы», специализации: «Радиоэлектронная борьба».

Второй под этап предполагает развертывание

- открытие специалитета по направлению подготовки «Информационная безопасность телекоммуникационных систем» (перспектива на 2021 г.);

Параллельно развитию системы подготовки высшей профессиональной подготовки по ИБ в университете активно развивается и система подготовки средней профессиональной подготовки базе Колледжа космического машиностроения и технологий.

В частности, в 2016 году осуществлен набор студентов по направлению подготовки «Организация и технология защиты информации» и «Информационная безопасность инфокоммуникационных систем» по специальности «техник по защиты информации». При этом, выпускники колледжа имеют возможность продолжить свое образование по направлению «Информационная безопасность» в Технологическом университете» как по очной, так и по очно-заочной форме обучения.

Данное положение в полной мере соответствует и для выпускников колледжа по направлению «Радиоэлектронные системы и средства», специальность «Радиотехник». С 2019 г. они имеют возможность продолжить свое образование в МГОТУ по специализации «Радиоэлектронная защита/радиоэлектронная борьба», либо по «Радиоэлектронные системы космических комплексов».

При этом, указанные направления подготовки кадров по ИБ будут опираться на существующие международные стандарты по ИБ, что позволит обеспечить дальнейшее сближение процесса обучения студентов по ИБ с учебными заведениями ведущих иностранных государств.

В заключении к изложенному следует указать ряд проблемных вопросов по развитию системы подготовки кадров по информационной безопасности в Технологическом университете в тесной взаимосвязи с ведущими иностранными учебными заведениями. Данные вопросы целесообразно объединить по двум группам.

Первая группа - это вопросы, требующие дополнительной поддержки (финансовой, материальной и т.д.):

закупка и оснащение современной учебно-научной (лабораторной) материально-технической базы;

выделение дополнительных учебно-производственных площадей (служебных помещений).

Вторая группа - это вопросы, решаемые в основном силами Технологического университета:

подбор и обучение профессорско-преподавательского состава и сотрудников;

получение соответствующих лицензий для проведения вышеуказанных специальных работ в области информационной безопасности;

использование международных нормативно-методических документов по обеспечению информационной безопасности;

активизация работ по профессиональной ориентации в области ИБ выпускников средних школ и заведений СПО региона в интересах заблаговременной подготовки и отбора абитуриентов.

Таким образом, в данной статье рассмотрены вопросы, связанные с необходимостью и целесообразными направлениями развития существующей системы подготовки профессионалов в области информационной безопасности на базе Московского государственного областного технологического университета (г. Королев) для региона Московской области. Данная задача обусловлена высокой востребованностью специалистов в области информационной безопасности, как в настоящее время, так и в будущем с учетом развития современного информационного общества. Имеющийся сформированный потенциал МГОТУ в рассматриваемой области позволит участвовать в совместной подготовке профессиональных кадров по ИБ в современном международном образовании.

Список использованных источников:

1. Федеральный закон Российской Федерации: «Об образовании» (от 29 декабря 2012 г. №273);
2. Распоряжение Правительства РФ от 03.11.2011 № 1944-р «О перечне направлений подготовки (специальностей) в образовательных учреждениях высшего профессионального образования, специальностей научных работников, соответствующих приоритетным направлениям модернизации и технологического развития российской экономики» Официальная публикация в СМИ: "Российская газета", № 254, 11.11.2011 "Собрание законодательства РФ", 14.11.2011, № 46, ст. 6584
3. Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 10.03.01 Информационная безопасность (квалификация (степень) «бакалавр»), утвержденный приказом Министерства образования и науки Российской Федерации от «01» декабря 2016 г. № 1515 (Зарегистрировано в Минюсте России 20 декабря 2016 года № 44821) (далее - ФГОС ВО);
4. Развитие цифровой экономики в России (Программа развития цифровой экономики до 2035 года) Утв. распоряжением Правительства РФ от 28 июля 2017 г. №1632-Р. (https://alterozoom.com/documents/38087.html обращение 11.11.2019 г.)
5. Соляной В.Н., Сухотерин А.И., Выработка коммуникативной компетенции при подготовке профессионалов по информационной безопасности с использованием

технологии модерации. «Инновационные технологии в современном образовании» [Текст] сборник трудов по материалам III Международной научно-практической Интернет-конференции 18 декабря 2015 г.–М.: Издательство «Научный консультант», 2016.–784с. (с.635-640). ISBN: 978-5-9907976-9-7В

6. Соляной В.Н., Сухотерин А.И., Антоненко В.И. Проблемно-ориентированная подготовка специалистов по информационной безопасности с использованием имитационного метода (мозговой штурм). «Инновационные технологии в современном образовании» [Текст] сборник трудов по материалам III Международной научно-практической Интернет-конференции 18 декабря 2015 г.–М.: Издательство «Научный консультант», 2016.–784с. (с.640-645). ISBN: 978-5-9907976-9-7В

7. Соляной В.Н., Сухотерин А.И Рекомендации по практике применения традиционных (неимитационных) методов и технологий образовательного процесса (практические занятия и лабораторные работы) в (учебный процесс) подготовку бакалавров (специалистов) и магистров по информационной безопасности «Инновационнные технологии в современном образовании» [Текст] сборник – Королев МО: Изд-во «Алькор Наблишерс», ФТА, 2015. – 456 с. (с.348-355).

8. Соляной В.Н., Сухотерин А. И., Антоненко В.И. Особенности практико-ориентированной (квазипрофессиональной) подготовки специалистов по информационной безопасности: деловая игра – имитационный метод организации образовательного процесса «Инновационнные технологии в современном образовании» [Текст] сборник – Королев МО: Изд-во «Алькор Наблишерс», ФТА, 2015. – 456 с. (с.355-360).

9. Соляной В.Н., Сухотерин А.И. Практика применения инновационного научно-образовательного комплекса по подготовке бакалавров и магистров в области информационной безопасности. Научно-практический журнал №25, том 1 2015г. ИНФОРМАЦИОННОЕ ПРОТИВОДЕЙСТВИЕ УГРОЗАМ ТЕРРОРИЗМА. **Материалы** XIX ПЛЕНУМА УЧЕБНО-МЕТОДИЧЕСКОГО ОБЪЕДИНЕНИЯ ПО ОБРАЗОВАНИЮ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ «ОПЫТ И ПЕРЕДОВЫЕ ПРАКТИКИ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ ПО ФОРМИРОВАНИЮ И ИСПОЛЬЗОВАНИЮ В УЧЕБНОМ ПРОЦЕССЕ СПЕЦИАЛИЗИРОВАННОЙ УЧЕБНО - ЛАБОРАТОРНОЙ БАЗЫ» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН. ФЕД.УНИВ, 2015.-416 с. (с. 359-367) ISSN 2219-8792.

10. Соляной В.Н., Сухотерин А.И. Модульно – ориентированный подход формирования базовых дисциплин ФОС 3+ как основа реализации профессиональной подготовки бакалавров в области информационной безопасности. Научно-практический журнал №25, том 2 2015г. ИНФОРМАЦИОННОЕ ПРОТИВОДЕЙСТВИЕ УГРОЗАМ ТЕРРОРИЗМА. **Материалы** XIX ПЛЕНУМА УЧЕБНО-МЕТОДИЧЕСКОГО ОБЪЕДИНЕНИЯ ПО ОБРАЗОВАНИЮ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ «УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» г. Таганрог. РОСТ. ОБЛ.: Изд-во ЮЖН. ФЕД.УНИВ, 2015.-330 с. (с.249- 255) ISSN 2219-8792