

Секция «Проблемы компьютерного права и информационной безопасности»

Подготовка IT-юриста к работе в информационной сфере

Научный руководитель – Батурин Юрий Михайлович

Де Апро Сона Вагановна

Студент (магистр)

Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Кафедра информационной безопасности и компьютерного права, Москва, Россия

E-mail: s.deapro@yandex.ru

Сегодня цифровая экономика активно внедряется в жизнь страны. В 2017 году Правительство разработало и утвердило программу перехода страны к цифровой экономике[n1], которая представляет собой деятельность, неразрывно связанную с цифровыми технологиями. В «Стратегии развития информационного общества РФ на 2017-2030 годы» цифровая экономика определяется следующим образом: «Цифровая экономика - это хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг»[n2].

Также была утверждена Стратегия развития информационного общества на 2017-2030 годы. Следовательно, требуются регулирующие подходы и введение новых специальностей для экономического и финансового контроля в информационной среде.

Существующая проблема нехватки кадров в информационной среде обсуждалась главами финансовых корпораций на Петербургском международном экономическом форуме в мае 2018 года. На Пленарном заседании Международного конгресса по кибербезопасности в июле 2018 года Президент РФ В.В. Путин отметил, что ключевой задачей программы «Цифровая экономика Российской Федерации» является «подготовка профессиональных кадров, формирование компетенций, которые позволят вести дальнейшие масштабные преобразования в области цифровой экономики»[n3].

По данным исследований[n4], проведенным в сфере кибербезопасности, к 2022 году ожидается дефицит около 1,8 миллиона специалистов по кибербезопасности, причем из них около 75% являются действующие работники, квалификация которых уже к тому моменту не будет соответствовать необходимому уровню для выполнения своих обязанностей.

Сегодня практикующие и будущие юристы, как и специалисты многих других сфер, нуждаются в приобретении технологических навыков, которые помогут им адаптироваться к новым реалиям. Новые технологии вместе с вполне положительными функциями внесли в жизнь ряд проблем, связанных с безопасностью пользователей, их электронной деятельностью, работой организаций, использующих цифровые технологии и электронные данные. Все это попадает под угрозу мошенничества, взлома, вирусов и т.д. В связи с этим необходим более творческий и инновационный подход в обучении юристов в XXI веке, в их подходе к профессиональной деятельности.

Россия заняла второе место в рейтинге стран по количеству кибератак вслед за США, по оценкам экспертов международной компании Positive Technologies[n4], специализирующейся на разработке программного обеспечения в области информационной безопасности. Основной целью злоумышленников является финансовая выгода, меньше всего атак из-за политики. Согласно исследованию компании Positive Technologies, финансовая выгода

стала мотивом для 71% атак, на кибершпионаж пришлось 20% кибератак, на «хактивизм» (компьютерный терроризм) — 6%. Доля атак, целью которых является кибервойна (нанесение ущерба в политических интересах той или иной страны), составила всего 3%.

Согласно докладу Всемирного экономического форума о глобальных опасностях наступившего года [п5], в среди главных мировых рисков - усиление геополитических и экономических разногласий между крупными государствами, состояние окружающей среды, распространение оружия массового поражения и крупномасштабные кибератаки, кража данных и кибермошенничество. Уязвимость технологической инфраструктуры становится все более серьезной проблемой для национальной безопасности стран.

Предлагается ввести понятие «IT-юриста», которое подразумевает взаимодействие права и технологий. Данный термин широко распространен в англоязычной юридической литературе, что подтверждает актуальность существующей проблемы кадров в информационной сфере. Информационная безопасность работы аудитора в информационной среде может пониматься как в глубоком понимании аудитором информационной среды и безошибочной (по возможности) его работы в ней, так и в защите аудиторских операций в информационной среде от внешних воздействий.

Первостепенной задачей «IT-юриста» является углубленное ознакомление с видами преступности, существующими в информационной среде, способами их совершения для того, чтобы определить степень их опасности и методы их проверки и устранения. В перечень профессиональных компетенций «IT-юриста» должны входить: умение использовать необходимые технические ресурсы, ПО; знание о современных преступных группировках, теневой стороны сети Интернет; способность общаться с техническими специалистами, например, в области анализа вредоносного кода, знание судебной практики и т.д.

Таким образом, цифровое пространство стремительно усложняется, и цифровизация меняет подход к профессиональной деятельности, что требует введения и подготовки новых специалистов. Аудит в электронной области проникает во все сферы жизни, вскрывая зоны, недоступные для традиционного контроля. Новые технологии и потребность постоянной работы с интернет-инновациями и глобальной сетью в целом приводят к необходимости их контроля и регулирования самой деятельности, ведущейся с помощью них, а следовательно, требуются новые формы и методы аудита для разрешения возникающих в информационном пространстве проблем, несущих угрозу для государства, крупных корпораций и для граждан. Нормативно-правовая база работы аудиторов и юристов в сфере IT нуждается в дополнении в части установления правил контроля операций, использующих новые информационные технологии.

Источники и литература

- 1) Официальный сайт Правительства России/ <http://static.government.ru>
- 2) Указ Президента Российской Федерации от 09.05.2017 г. № 203/ Официальный сайт Президента России/ <http://kremlin.ru/acts/bank/41919>
- 3) Пленарное заседание Международного конгресса по кибербезопасности/ Официальный сайт Президента России/ <http://kremlin.ru/events/president/news/57957>
- 4) Официальный сайт компания по разработке программного обеспечения «Positive Technologies»/ <https://www.ptsecurity.com>
- 5) Отчет по глобальным рискам/ Официальный сайт Всемирного экономического форума/ <http://reports.weforum.org/global-risks-2018/>