УДК 004.056

Корх И. А., Юмашева Е. В.

ЦИФРОВИЗАЦИЯ И АКТУАЛЬНЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ирина Анатольевна Корх
kiiz_org@inbox.ru,
НЧОУ ВО «Кубанский Институт информзащиты», Краснодар, Россия,
Юмашева Елена Всеволодовна
кандидат экономических наук, доцент
umashevaev@mail.ru
НЧОУ ВО «Кубанский Институт информзащиты» Краснодар, Россия

DIGITALIZATION AND CURRENT THREATS TO INFORMATION SECURITY

Korkh Irina Anatolyevna,
NCHOU VO «Kuban Institute of Information Protection», Krasnodar, Russia
Yumasheva Elena Vsevolodovna
Candidate of Economic Sciences, Associate Professor,
NCHOU VO «Kuban Institute of Information Protection» Krasnodar, Russia

Аннотация. *В статье актуализирован перечень угроз информационной безопасности, связанных с феноменом цифровизации. Поднят вопрос подготовки кадров в сфере информационной безопасности с учетом геополитической обстановки. Рассмотрены гуманитарные и социотехнические аспекты повышения осведомленности в вопросах безопасности информации для сотрудников организаций. Авторами предложен перечень мероприятий, реализация которых позволит поддерживать на должном уровне защищенность личности, общества и государства от деструктивного информационного воздействия и недопущения реализации информационных угроз.*

Ключевые слова: *цифровизация; угрозы информационной безопасности; гуманитарные аспекты информационной безопасности; повышение осведомленности; уязвимости.*

Annotation. *The article updated the list of threats to information security associated with the phenomenon of digitalization. The issue of training personnel in the field of information security was raised, taking into account the geopolitical situation. The humanitarian and socio-technical aspects of raising awareness of information security issues for employees of organizations are considered. The authors propose a list of measures, the implementation of which will allow maintaining at the proper level the protection of the individual, society and the state from the destructive information impact and preventing the implementation of information threats.*

Keywords: *digitalization; information security threats; humanitarian aspects of information security; raise awareness; vulnerabilities.*

Развитие информационных технологий привело к существенным изменениям во всех областях и сферах жизни общества. Преобразование информации в цифровую форму, позволяющую ускорять обмен, доступность и защищенность информации, автоматизацию процессов, способствует повышению эффективности экономики и качества жизни людей в контексте их социализации и коммуникации. Цифровизация не могла обойти стороной и систему подготовки кадров в этой сфере. Высшее образование также подвергается изменению в части наполнения учебных дисциплин, а также методов и методик их преподавания. Направления подготовки, связанные с информационными технологиями и информационной безопасностью, находятся в тренде у абитуриентов уже не один год. Однако, стоит отметить, что осознанный выбор делают только 30 % всех поступающих в региональные высшие учебные заведения. Также озабоченность вызывает малое количество технических специалистов, для которых гуманитарные аспекты информационной безопасности имели бы соизмеримую важность с сетевой и кибербезопасностью. Особый интерес

представляет изучение влияние цифровизации на гуманитарные и социотехнические аспекты преподавания дисциплин по информационной безопасности в технических вузах.

Цифровизация сегодня рассматривается как тренд эффективного мирового развития [1], охватывающий все сферы деятельности человека, начиная с экономики, образования, науки, культуры и заканчивая такими, казалось бы, не цифровыми отраслями, как транспорт, сельское хозяйство, социальное обслуживание и другие. В случае эффективного использования ее результатов, жизнь гражданина, производственный процесс промышленных предприятий, развитие общества и государства в целом, выходят на новый уровень. Однако большие права и возможности приводят к соизмеримым проблемам и ответственности. Закон причин и следствий иллюстрирует, что повышение доступности сведений об объектах обязательно приведет к увеличению числа создаваемых баз данных. Руководители и представители юридических лиц не всегда отдают отчет в целесообразности сбора и обработки хранимой в них информации, что приводит зачастую к бесконтрольному ее копированию — резервированию, якобы для целей организации. Контроль за законным использованием таких ресурсов не приносит прибыли, потому часто не ведется на должном уровне. Сотрудники часто подвергаются воздействию методами социальной инженерии, но повышение осведомленности не входит в тренд для подавляющего большинства организаций. Исключение составляют банковские учреждения, объекты критической инфраструктуры топливно-энергетического комплекса, однако нельзя связать эту тенденцию с желанием работодателя, скорее с нормативным регулирование данных вопросов и жесткими санкциями при невыполнении требований. Специалисты по защите информации в организациях хорошо справляются с угрозами технического характера, но оказываются практически беспомощны в вопросах защиты от угроз, связанных с гуманитарными аспектами цифрового общества.

Любые изменения, происходящие в обществе, кроме желания его членов, основываются на потребностях государства в таких изменениях. Так,

цифровая трансформация российского общества регламентируется некоторыми нормативными документами [2–6]. Вышесказанное позволяет сделать вывод о том, что цифровизация и новые угрозы информационной безопасности привели к необходимости смещения фокуса внимания от технических каналов утечки к гуманитарным, позволяющим предотвратить пагубное влияние атак социальной инженерии на личность человека.

Несмотря на все положительные тенденции развития мирового сообщества цифровизация сопряжена с новыми рисками, вызовами и угрозами для национальной и международной информационной безопасности. Сегодня мы являемся свидетелями, как не только отдельные злоумышленники, преступные сообщества террористов и экстремистов, но и целые государства используют возможности современных информационных технологий в целях проведения террористических, экстремистских, военных, криминальных и иных противоправных атак, направленных на уничтожение и подрыв государственности.

В этой связи, считаем целесообразным включение в программу бакалавриата по направлению 10.03.01 дисциплины «Введение в специальность», а всех остальных направлений «Гуманитарные аспекты информационной безопасности» на первом курсе вместо «Основ информационной безопасности» для повышения осознанности в выборе будущего направления деятельности специалистов по защите информации и общего повышения осведомленности в вопросах возможного влияния на личность методами социальной инженерии. Исследования по вопросу повышения осведомленности были поддержаны Грантом ФУМО по УГСН 10.00.00 «Информационная безопасность».

Применение цифровых технологий в повседневной жизни, как уже было сказано выше, приводит к повышенной уязвимости не только данных, но и конечных пользователей ресурсов. На первый план выходит способность человека противостоять недостоверной, откровенно фейковой информации, транслируемой информационными ресурсами. Наибольшую опасность вызывает

неспособность принятия верного решения профильными специалистами отделов мониторинга и информационной безопасности, а также первых лиц учреждений, предприятий и организаций. Кибератаки за последние 2 года изменили профили и вектора, что приводит к необходимости учета этих изменений при подготовке специалистов.

По данным МИД в 2022 году в РФ были успешно ликвидированы более 25 тыс. кибератак на госресурсы и 1,2 тыс. инцидентов на объектах критической инфраструктуры. Число кибератак в 2022 году возросло более, чем на 80 %, основной удар принял на себя госсектор. Большинство кибератак осуществлялось странами НАТО и ЕС, а также Украины, что обусловлено в том числе проведением специальной военной операции [7]. За период с 2017 по 2023 годы количество преступлений в компьютерной сфере РФ выросло в 12 раз. Аналитика данного факта представлена на основании статистической информации Генеральной прокуратуры, причем удельный вес таких преступлений вырос до 25,8 %, а чаще всего преступления совершаются с использованием сети Интернет и мобильных устройств, что косвенно подтверждает увеличение атак не на организацию, а на конкретных людей и не последнюю роль в данных преступлениях занимают методы социальной инженерии [8].

Уязвимость информации в условиях цифровизации провоцирует угрозу критической информационной инфраструктуры, приводит к снижению конкурентоспособности страны, дополнительным финансовым издержкам, связанным с восстановлением информации, сбоям функционирования организаций и социальной сферы и национальной безопасности государства.

Раскрываемость киберпреступлений также оставляет желать лучшего, поскольку квалификация специалистов правоохранительных органов не всегда соответствует необходимому для этого уровню, а также несовершенством правовой системы информационного права, что подтверждается независимой экспертизой данного параметра адвокатским сообществом [9].

К основным угрозам информационной безопасности в условиях глобальной цифровизации можно отнести:

- высокий уровень технологической зависимости РФ от других стран. Применяемые информационные технологии как правило являются заимствованными иностранными решениями. По отдельным направлениям информационной безопасности доля зарубежных решений достаточна велика: иностранные системы по защите от целевых атак составляют до 65 % рынка в стране, решения для защиты корпоративной почты — до 70 %, [10]. Разработчики в случае выявления уязвимостей не всегда своевременно выпускают необходимые обновления. По данным исследования Security Navigator 2021 выявленные проблемы решались в течение 7–56 дней только в менее 19 % случаев, от 31 до 180 дней — почти в 57 % случаев, в 14 % случаев исправления появлялись более чем через полгода. Задержки в исправлении уязвимостей играют в пользу злоумышленников, позволяя взламывать и использовать в своих целях продукты безопасности [11];
- невозможность обеспечения защиты значимых сфер жизни общества. Создание средств информационной безопасности кардинально отстает от современных темпов глобальной цифровизации. Внедрение технологий, не имеющих надежной защиты, ведет порой к необратимым последствиям;
- недостаточный контроль защиты систем сбора, обработки, хранения и передачи информации в виду большого количества зарубежных структур и высокая возможность несанкционированного доступа с целью противоправного копирования информации, ее искажения (вследствие случайных или преднамеренных нарушений требований работы с информацией);
- недостаток качественных специалистов в отделах мониторинга коммерческих организаций и технических специалистов правоохранительных органов, имеющих необходимые компетенции для адекватного реагирования на угрозы и расследования уже произошедших правонарушений;
- не соответствие системы правового регулирования современным требованиям в области обеспечения информационной безопасности. Совре-

менные угрозы, связанные с использованием искусственного интеллекта и робототехники, приводящие к преступным последствиям, обуславливают необходимость в системной модернизации информационного права;

- отсутствие на законодательном уровне со стороны регуляторов требований о необходимости защиты от угроз информационной безопасности, направленных на человека, как наиболее подверженного воздействию узла любой информационной системы.

Обеспечение информационной безопасности часто регламентируется нормами международного права, поскольку в России ряд информационно-правовых вопросов не решен на законодательном уровне в национальной системе права. В этой связи информационная война, которая проводится в настоящее время в отношении Российской Федерации имеет правовую оценку двойных стандартов.

Обеспечение информационной безопасности в условиях цифровой трансформации возможно, на наш взгляд, при условии:

- модернизации нормативно-правовой базы в сфере информационного права в соответствии с современными вызовами и угрозами информационной безопасности;
- перехода на отечественное программное обеспечение всех объектов критической инфраструктуры, поддержки отечественного производителя в сегменте разработки средств защиты, программного и технического оснащения, а также средств контроля качества безопасной разработки, восстановление практики научно-исследовательских и конструкторских бюро при федеральных Вузах и учебных заведениях инженерной и технической направленности, повышения вовлеченности государства в процесс импортозамещения отрасли высоких технологий;
- совершенствования системы подготовки кадров и методов отбора специалистов в области информационной безопасности, повышение информационной грамотности населения в контексте защиты информации, соблюдение кибергигиены всеми субъектами отношений;

- внедрения самостоятельных и независимых средств мониторинга обеспечения информационной безопасности, постоянное совершенствование технических и организационно-технических систем контроля уровня защищенности в условиях изменяющегося ландшафта информационных угроз;
- повышения общей сознательности всех пользователей информационных систем и осведомленности в вопросах информационной безопасности для целей поддержания необходимого уровня защищенности личности, общества и государства, защиты населения от деструктивного информационного воздействия и недопущения реализации информационных угроз.

Материалы исследования при финансовой поддержке Минобрнауки России (Грант ИБ) № 26/2020

Список литературы

1. *Халин, В. Г.* Цифровизация и ее влияние на российскую экономику и общество: преимущества, вызовы, угрозы и риски / В. Г. Халин, Г. В.Чернова. Текст: электронный // Управленческое консультирование. 2018. № 10 (118). С. 46–63. https://doi.org/10.22394/1726-1139-2018-10-46-63.

2. *Стратегия* развития информационного общества в Российской Федерации на 2017–2030 годы: утверждена Указом Президента РФ от 9 мая 2017 г. № 203. Текст: электронный // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_216363/e91cc5f89aaced60e19c6c6554fc03432f4ee971/ (дата обращения: 18.02.2023).

3. *Программа* «Цифровая экономика Российской Федерации»: утверждена Распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р. Текст: электронный // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_221756/2369d7266adb33244e178738f67f181600cac9f2/#dst100006 (дата обращения: 18.02.2023).

4. *Об утверждении* типового положения о заместителе руководителя организации, ответственного за информационную безопасность и о структурном подразделении информационной безопасности: Постановление Правительства РФ от 15 июля 2022 № 1272. Текст: электронный // Гарант. URL:

https://base.garant.ru/405015639/?ysclid=lhv1ovfx55639020995 (дата обращения: 18.02.2023).

5. *Поручение* Президента Российской Федерации от 6 декабря 2022 № Пр–2330 «О совершенствовании подготовки кадров для обеспечения информационной безопасности РФ». Текст: электронный // Гарант. URL: https://www.garant.ru/products/ipo/prime/doc/405792441/?ysclid=lhv1tdliwj982412270 (дата обращения: 18.02.2023).

6. *Об утверждении* Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей: Указ Президента Российской Федерации от 09.11.2022 № 809. Текст: электронный // Официальный сайт Президента России. URL: http://www.kremlin.ru/acts/bank/48502 (дата обращения: 18.02.2023).

7. *МИД*: IT-инфраструктура России позволяет эффективно противодействовать кибератакам. Текст: электронный // ТВ-Новости. 2022. 28 дек. URL: https://russian.rt.com/russia/news/1091654-mid-rossiya-kiberataka (дата обращения: 18.02.2023).

8. *Состояние* преступности в России // Портал правовой статистики. URL: http://crimestat.ru/analytics (дата обращения: 18.02.2023). Текст: электронный.

9. *Киберпреступлений* становится все больше, однако их раскрываемость уменьшается. Текст: электронный // Адвокатская газета. 2018. 13 нояб. URL: https://www.advgazeta.ru/novosti/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvaemost-umenshaetsya (дата обращения: 18.02.2023).

10. *Западные* системы защиты от целевых кибератак до марта занимали до 65 % рынка в РФ – эксперт. Текст: электронный // Financial One: журнал о финансовых рынках. 2022. 4 июля. URL: https://fomag.ru/news-streem/zapadnye-sistemy-zashchity-ot-tselevykh-kiberatak-do-marta-zanimali-do-65-rynka-v-rf-ekspert/ (дата обращения: 16.02.2023).

11. *Золотова, Т.* Цифровая трансформация и риски безопасности. URL: https://telesputnik.ru/materials/tech/article/tsifrovaya-transformatsiya-i-riski-bezopasnosti (дата обращения: 10.02.2023). Текст: электронный.