доброжелательный ответ, направленный на улучшение творчества автора. Здесь работа идет по-прежнему плодотворно.

Во втором случае автор и редактор прекрасно знают друг друга как людей со своими достоинствами и недостатками, однако зачастую они не имеют ни малейшего понятия о том, как работать друг другом. Не получится ли высказывание по поводу нового произведения слишком жестким и не обидится ли на это друг? Не приведет ли это к неожиданному ухудшению дружбы и последующему разрыву? Не окажется ли, что по поводу творчества и его редактирования у них совершенно разные мысли и что лучше отказаться от всяких попыток работать вместе? Здесь существуют разные конфликты и такие же разные решения этих конфликтов, и стоит рассматривать каждый отдельный случай, чтобы сформировать полное представление о подобном типе отношений автора и редактора.

Вывод. От понимания между автором и редактором зачастую зависит итоговое качество текста. Чем лучше автор и редактор сработаются, чем плодотворнее будет их сотрудничество, тем выше вероятность коммерческого и профессионального успеха произведения, которое затем будет опубликовано в интернет-пространстве.

Список использованных источников

1. Рунету 25 лет: экспериментальный нет-арт, сетература и чатик «Кроватка» // Strelka Magazine [Электронный ресурс]. URL: https://news.rambler.ru/other/42015368-runetu-25-let-eksperimentalnyy-net-art-seteratura-i-chatik-krovatka/ (дата доступа: 01.12.2019)

2. Корректор // Издательский словарь-справочник [Электронный ресурс] / А. Э. Мильчин. – 3-е изд., испр. и доп. – М.: ОЛМА-Пресс, 2006.

УДК 004.056

П.П. Урбанович
Белорусский государственный технологический университет

КИБЕРПРОСТРАНСТВО: ТРЕНДЫ, УГРОЗЫ И БЕЗОПАСНОСТЬ

Нынешнее тысячелетие характеризуется масштабными изменениями в области информационно-коммуникационных технологий (ИКТ). Эти изменения касаются трансформации основных сторон жизнедеятельности как отдельных людей, отдельных государств, так и международного сообщества в целом.

Глобализация и виртуализация привели к появлению угроз и вызовов, которые принято связывать с киберпространством и кибербезопасностью (КБ). Эту новую реальность необходимо рассматривать и оценивать как стратегическую проблему государственной важности, затрагивающую все слои общества.

Известно устоявшееся (возможны несущественные вариации) определение информационной безопасности (ИБ) [1]. Основными целями обеспечения ИБ являются конфиденциальность, целостность и доступность. По аналогии с распространенным определением ИБ под кибербезопасностью понимают свойство и состояние системы с точки зрения защищенности различных компонент этой системы (информация, каналы связи, аппаратные и программные средства и др.) от угроз нарушения конфиденциальности, целостности, доступности в некоторой абстрактной, виртуальной среде – киберпространстве. На рис. 1 представлена взаимосвязь понятий в предметной области на основе положений стандарта ISO 27032.

Важнейшей из указанных целей обеспечения ИБ является конфиденциальность, которую нужно рассматривать не только в отношении информации, но также в отношении прав человека и организаций на неприкосновенность частной жизни, защиту персональных данных. Кроме того, понятие границ в виртуальной среде (или в цифровом киберпространстве) является условным, а сами границы – достаточно легко преодолимым препятствием. Вместе с тем, в разных странах определение рассматриваемых понятий может значительно различаться. Как следствие, различаются и подходы в разработке политики ИБ и КБ. Например, США разработали стратегию для киберпространства еще в 2011 году [2]. Эта стратегия определена как международная и содержит описание и целеуказания по семи направлениям в рамках сотрудничества между правительством, международными организациями и структурами, а также частным сектором:

- экономика (разработка и продвижение международных стандартов, открытость рынков),
- защита сетей (безопасность и надежность),
- правопорядок (расширение сотрудничества в правовой сфере),
- военная отрасль (анализ вызовов безопасности и реагирование на них),
- цифровое (Интернет) правительство,
- международное взаимодействие и развитие,
- свобода в Интернете (поддержка основных свобод и неприкосновенности частной жизни).

Рис. 1 – Взаимосвязь понятий в области кибербезопасности

Отсутствие общего подхода и даже общего понимания проблемы усложняет процесс международного сотрудничества в рассматриваемой области, тогда как важность сотрудничества признается всеми странами. В этой связи и в контексте развития событий особую остроту приобретает гармонизация национальных и международных правовых норм в сфере ИКТ [3]. На важность и остроту проблемы указывают соответствующие решения Организации Объединенных Наций. Например, Резолюция Генеральной ассамблеи ООН от 3 декабря 2012 г. [4].

Результаты многочисленных исследований в области ИБ показывают, что вопросы КБ занимают все больше места в «повестке дня» различных корпоративных мероприятий ученых и специалистов, государственных чиновников, включая высших должностных лиц, после ряда масштабных атак и ряда взломов существующих систем защиты со стороны хакерских групп, финансируемых, по утверждениям, на государственном уровне.

Национальные программы в области ИКТ (в том числе – и в РБ), соответствующие ведомственные программы, программы развития ИТ-компаний предусматривают расширение внедрения роботизации, машинного обучения, искусственного интеллекта, блокчейна, облачных технологий, Интернета вещей и т.п. Все это влечет за собой дополнительные киберриски, которые оборачиваются многомиллиардными потерями компаний. По данным [5] в 2018 году на Россию было совершено более 4,3 миллиарда кибератак на критическую информационную инфраструктуру.

Не только в теории можно удаленно и несанкционированно управлять любым транспортным средством (автомобиль, корабль, самолет, поезд), или даже взломать систему защиты сервера центра по работе с компонентами атомных электростанций или ядерного оружия. Растет число ботнетов (сетей компьютеров, которые управляются хакерами удаленно), что связано, в том числе, с ростом числа смарт-устройств и их слабой защищенностью. Некоторые из ботнетов наделяются признаками искусственного интеллекта. Приобретает угрожающие размеры воровство персональных данных из «облаков» [6], воровство с использование платформ для многоплеерных компьютерных игр [7], различных вирусов-вымогателей. Обсуждаются расклады по «национальным» группировкам хакеров. Таким образом, кибервойны становятся реальностью.

По информации [8] в настоящее время киберриски связаны, в основном, с несанкционированным доступом к информации экономического, научного или иного интеллектуального характера (см. табл. 1).

В табл. 2 приведена информации о рисках в киберпространстве, которые в последние несколько лет заметно возросли. Понятно, что нейтрализация таких угроз требует серьезных денежных средств. Осознанность компаний насчет кибератак медленно, но неуклонно растет. Как видно из табл. 2, ключевая проблема заключается в уровне базовых знаний сотрудников в области безопасности ИТ. За этим стоит еще более серьезная проблема – дефицит специалистов по кибербезопасности. Эта проблема актуальна и для Беларуси.

С учетом практически повсеместного использования web-ресурсов во всех организациях, необходимо повсеместно, начиная со средних школ, сформулировать цели информационных обучающе-тестирующих программ, призванных привить пользователям новые модели поведения и модели работы с интернет-ресурсами.

Таблица 1 – 10 наиболее ценных для злоумышленников типов данных

№ пп.	Тип данных	Среднее количество атак, %
1	Клиентская информация	17,0
2	Финансовая информация	12,0
3	Стратегические планы	12,0
4	Информация о высшем руководстве	11,0
5	Пароли клиентов	11,0
6	Результаты НИОКР	9,0
7	Информация о сделках	8,0
8	Объекты интеллектуальной собственности	6,0
9	Незапатентованная интеллектуальная собственность	5,0
10	Информация о поставщиках	5,0

Таблица 2 – Уязвимости, по которым связанные риски значительно возросли [8]

№ пп.	Тип данных	Численный показатель, %
1	Неосмотрительность/неосведомленность сотрудников	34,0
2	Устаревшие средства контроля безопасности	26,0
3	Несанкционированный доступ	13,0
4	Применение облачных технологий	11,0
5	Использование смартфонов/планшетов	8,0
6	Уязвимости, связанные с социальными сетями	5,0
7	Уязвимости, связанные с технологиями Интернета вещей	4,0
8	Объекты интеллектуальной собственности	6,0
9	Незапатентованная интеллектуальная собственность	5,0
10	Информация о поставщиках	5,0

Приведенные здесь, а также в других многочисленных информационных источниках сведения являются веским доказательством необходимости пересмотра программ образования с упором на обучение ИТ-специалистов и профессионалов в области кибербезопасности. Необходимы также всевозможные тренинги, улучшающие навыки пользователей и снижающие риски из-за их неосмотрительности или неосведомленности.

Список использованных источников

1. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие. – Минск: БГТУ, 2016. – 220 с.

2. [Электронный ресурс]: URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf , дата доступа: 13.10.2012.

3. Urbanowicz, P. Bezpieczenstwo w cyberprzestrzeni a prawo karne / P. Urbanowicz, M. Smarzewski // Ksiega pomiatkowa ku czci Księdza Profesora Andrzeja Szostka MIC, Lublin: KUL. – 2016. – P. 479–488.

4. Developments in the field of information and telecommunication in the context of international security, [Электронный ресурс]: URL: http://research.un.org/en/docs/ga/quick/regular/67, дата доступа: 26.11.2019.

5. [Электронный ресурс]: URL: https://rg.ru/2018/12/12/za-god-na-rossiiu-bylo-soversheno-bolee-chetyreh-milliardov-kiberatak.html, дата доступа: 26.11.2019.

6. Гладкий, М. В. Безопасность приложений на платформах облачных вычислений / М. В. Гладкий, П. П. Урбанович // Информационные технологии: тезисы 79-й науч.-техн. конф. профессорско-препод. состава, научн. сотрудников и аспирантов (с междунар. участием), Минск, 2–6 февраля 2015г. – Минск: БГТУ, 2015. – С. 18–19.

7. Błaszczak, M. Server security of the multiplayer game «PROJECT I.G.I. 2: COVERT STRIKE» / M. Błaszczak, P. P. Urbanovich // Информационные технологии : материалы 83-й научно-техн. конф. профессорско-препод. состава, научн. сотр. и аспирантов, Минск, 4–15 февраля 2019 г. – Минск: БГТУ, 2019. – С. 117–119.

8. Кибербезопасность: больше чем защита?, [Электронный ресурс]: URL: https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-rus/%24FILE/ey-global-information-security-survey-rus.pdf, дата доступа: 15.11.2019.

УДК 004.41:330.123.6

Т. Фалалеева
Издательство «Регистр»

ГЛОБАЛЬНАЯ ЦИФРОВАЯ ТРАНСФОРМАЦИЯ: ГЛУБОКОЕ ПЕРЕОСМЫСЛЕНИЕ И ПЕРЕСТРОЙКА ОТРАСЛИ УСЛУГ

Стремительное внедрение в экономическую деятельность результатов научно-технического прогресса, а также разработка принципиально новых бизнес-моделей производства и поставки потребителям обусловили лидерство в современной мировой экономике отрасли услуг.

И если до недавнего времени большая часть видов услуг требовала наличия в непосредственной близости их производителей и потребителей, то сегодня благодаря тенденции глобальной цифровизации торговать услугами становится значительно проще. Трансграничная торговля услугами открывает новые возможности для национальных экономик.

По оценкам экспертов, объемы мировой торговли услугами достигли в 2018 г. рекордных 11,3 трлн дол. США[21]. Торговля росла в среднем на 6,1% в год с 2010 по 2018 годы, причём темпы роста торговли услугами опережали среднегодовые темпы роста торговли товарами, которые в этот же период времени составляли около 3,5%.

Так, за период с 2005 г. по 2017 г. в мире примерно 55% прямых иностранных инвестиций было направлено в отрасль услуг.

Дистрибьюторские и финансовые услуги являются наиболее торгуемыми услугами по всему миру. Каждый из этих подсекторов составляет примерно 1/5 часть в общем объеме мировой торговли услугами. Исследования и разработки зафиксировали самый быстрый среднегодовой рост за период с 2005 по 2018 годы (около 10%).

[21] Предварительная оценка.