Проблемы кибербезопасности в условиях цифровой трансформации экономики и общества

Cybersecurity issues in conditions of digital transformation of the economy and society

Головенчик Галина Геннадьевна, старший преподаватель кафедры международных отношений Белорусского государственного университета

Golovenchik Galina, senior lecturer, Department of International Relations, Belarusian State University
e-mail: goloventchik@bsu.by

Аннотация

В статье рассматривается такая глобальная угроза обеспечению политической и экономической безопасности страны, как киберпреступность. Данный вид угрозы требует особого внимания в условиях цифровой трансформации всех сфер жизни и деятельности современного общества ввиду масштабов ее распространения, глубины и проблематичности противодействия. Проведен анализ деятельности государств по обеспечению национальной кибербезопасности, современного состояния международного сотрудничества в области обеспечения борьбы с киберпреступностью. Дается характеристика проблем и угроз в сфере кибербезопасности Республики Беларусь, предложены пути их решения.
Ключевые слова: интернет, информация, киберпреступность, кибербезопасность, стратегия, международное сотрудничество, рекомендации.

Abstract

The article deals with such a global threat to ensuring the political and economic security of the country, like cybercrime. This type of threat requires special attention in the conditions of digital transformation of all spheres of life and activity of modern society in view of the scale of its distribution as well as depth and problematic nature of the countermeasures. The analysis of the activities of states to ensure national cybersecurity and current state of international cooperation in the field of combating cybercrime has been carried out. The description of problems and threats in the sphere of cybersecurity of the Republic of Belarus is given. Ways of solving the abovementioned problems are proposed.
Keywords: Internet, information, cybercrime, cybersecurity, strategy, international cooperation, recommendations.

Поступила в редакцию / Received: 04.12.2018
Web: http:elibrary.miu.by/jornals!/item.eui/issue.2/article.4.html

Введение

В последние несколько лет за Беларусью в Европе и мире прочно закрепилась репутация ведущей ИТ-страны в Восточно-Европейском регионе. Направление разработки программного обеспечения существует в республике фактически с 1998 г. Однако ключевой «точкой отсчета», с которой началось развитие ИТ-сферы в Беларуси, считается сентябрь 2005 г., когда Декретом Президента Республики Беларусь «О Парке высоких технологий» была заложена законодательная основа для успешной работы белорусского аналога Кремниевой долины и привлечения инвестиций в отрасль разработки программного обеспечения.

Для Парка высоких технологий и в целом для белорусской ИТ-отрасли 2017 год стал знаковым. С принятием Декретов Президента № 7 «О развитии предпринимательства» и № 8 «О развитии цифровой экономики» в Беларуси начался новый этап экономического развития. Руководство страны ясно и четко определилось: ставка делается на развитие частного бизнеса, который должен развиваться в высокотехнологичных сферах цифровой экономики.

Развитию технологий цифровой экономики также посвящены два программных документа, принятые Советом Министров: «Стратегия развития информатизации в Республике Беларусь на 2016–2022 гг.» и «Государственная программа развития цифровой экономики и информационного общества на 2016–2020 гг.». Благодаря реформированию законодательства у Беларуси появился реальный шанс привлечь крупных инвесторов для цифровизации белорусской экономики.

Однако многие аспекты построения цифрового общества, последствия цифровизации отраслей экономики, государственных услуг, социальных отношений до сих пор не отражены в программных документах по построению в Республике Беларусь цифровой экономики. В связи с этим считаем нужным обратить внимание на те риски и угрозы, которые несет цифровизация экономики и общества.

1. Понятие кибербезопасности

Н.И. Касперская, глава Рабочей группы Программы «Цифровая экономика» по направлению «Информационная безопасность», к числу рисков внедрения цифровых технологий относит:

– навязываемое заимствование западных технологий;

– новые уязвимости, связанные со слежкой, потерей тайны личной жизни;

– захват отечественного рынка мощными транснациональными компаниями;

– потерю рабочих мест, рост безработицы, возникновение социальной напряженности;

– возникновение новых этических проблем, рост мошенничества в киберпространстве, снижение каче-

ства и ответственности принимаемых решений, рост социального отчуждения;

– исчезновение приватности, появление навязчивой рекламы, утечку персональных данных граждан за границу к ведущим иностранным игрокам (Amazon, Apple, Facebook, Google, Microsoft) [1].

Как закономерный итог, – вместо появления нового технологического уклада, цифровой экономики с новым лицом традиционной индустрии, сельского хозяйства и государственного управления – стадия цифровой колонизации, когда экономика управляется извне, служит чужим интересам.

По нашему мнению, среди рисков, которые несут цифровые технологии, укрупненно можно назвать технологический, социальный, политический риски, риск социальной, экологической и личностной деградации.

Особенно хотелось бы остановиться на рисках в области цифровой безопасности и защиты информации.

Процессы глобализации, в том числе глобализации информационно-коммуникационных технологий (далее – ИКТ), предоставляют неограниченные возможности для оказания воздействия на личность и общество. Одним из негативных последствий развития ИКТ является появление и развитие новой формы преступности – в сфере высоких технологий, или киберпреступности, когда компьютеры или компьютерные сети выступают в качестве объекта преступных посягательств, а также средства или способа совершения преступлений.

Понятие «киберпреступность» в настоящее время нередко используется как синоним термина «компьютерная преступность», которому в русскоязычной литературе отдается большее предпочтение. На взгляд В.А. Номоконова и Т.Л. Тропиной, термин «киберпреступность» (англ. *cybercrime* – преступность, сопряженная как с применением компьютеров, так и информационных технологий и сетей) шире, чем «компьютерная преступность» (англ. *computer crime* – преступления, совершаемые против компьютеров или компьютерных данных), и более точно отражает природу такого явления, как преступность в информационной среде [2, с. 47].

С понятием «киберпреступность» неразрывно связано понятие «киберпреступление». Наиболее полное определение, отражающее аспекты данного негативного явления, дается Д.Н. Карповой: «киберпреступление – это акт социальной девиации с целью нанесения экономического, политического, морального, идеологического, культурного и других видов ущерба индивиду, организации или государству посредствам любого технического средства с доступом в Интернет». Здесь по большому счету отражаются даже не юридические аспекты, а имеющиеся социально-экономические проблемы современного общества [3, с. 47].

Проблема киберпреступности особо актуализировалась в эпоху цифровой трансформации экономики и общества, когда появление и распространение интернета привело к формированию единого информационного пространства и глобальных коммуникационных гиперсистем, охвативших все сферы жизнедеятельности человека и государства.

Вместе с цифровой трансформацией традиционной экономики происходит трансформация информационной безопасности, под которой в Концепции национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575, понимается «…состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере» [4]. Объект защиты, понимаемый ранее как совокупность классифицированных данных, приобретает более сложное представление – как киберпространство, включающее не только данные, но и системы их передачи, обработки и хранения; системы управления; средства защиты; а также их динамически изменяющиеся взаимосвязи, составляющие определенную ценность. Сегментами киберпространства являются суперкомпьютеры, автоматизированные системы управления технологическими процессами (АСУ ТП), корпоративные и домашние сети, мобильные системы, облачные сервисы, социальные сети и даже бытовые устройства. Д.П. Зегжда и соавт. определяют «…киберпространство как глобальную сферу в информационном пространстве, представляющую собой взаимосвязанную совокупность инфраструктур и информационных технологий, включая интернет, телекоммуникационные сети, компьютерные системы, встроенные процессоры и контроллеры» [5, с. 4].

Таким образом, к понятию информационной безпасности, базирующейся на безопасности информационно-телекоммуникационных систем, добавилось понятие кибербезопасности, понимаемой в ISO/IEC 27032:2012, как «…условия защищенности от физических, духовных, финансовых, политических, эмоциональных, профессиональных, психологических, образовательных или других типов воздействий или последствий аварии, повреждения, ошибки, несчастного случая, вреда или любого другого события в киберпространстве, которые могли бы считаться не желательными» [6]. Иначе говоря, кибербезопасность – это набор принципов и средств обеспечения безопасности информационных процессов, подходов к управлению безопасностью и прочих технологий, которые используются для активного противодействия реализации киберугроз.

2. Характеристика мировой киберпреступности

Мир, подключенный к сети, открывает все новые возможности для международных киберпреступников. Автоматический анализ информационных запросов пользователей в интернете, данные с личных «умных» гаджетов, транзакции по банковским картам, электронная переписка и мессенджеры создают блок исчерпывающей информации о человеке, которую можно похитить и использовать в корыстных целях [7, с. 33].

Информационно-телекоммуникационная сфера является крайне привлекательной для преступников-интеллектуалов, поскольку специфика информационных технологий такова, что с их применением можно нанести весьма существенный ущерб достаточно быстро и внезапно, находясь при этом вне зоны географической (территориальной) и правовой досягаемости от конкретного места совершения преступления. Это затрудняет работу правоохранительных органов по нахождению и привлечению злоумышленников к юридической ответственности.

Основными причинами нарастающей киберопасности являются: масштабный характер производи-

мых хакерами атак, их трансграничность, быстрый рост профессионализма хакеров, осуществление ими атак в отношении многочисленных клиентов и многих кредитных учреждений; незнание и недооценка клиентами и пользователями имеющихся проблем в сфере информационной безопасности; нередкое отставание программного обеспечения безопасности кредитных учреждений, применяющих интернет-банкинг, от хакерских вызовов.

Преступления в киберпространстве особо опасны, поскольку они не являются очевидными, могут иметь как длящийся, так и одномоментный характер. Такие деяния трудно выявить, а совершившие их лица нередко остаются безнаказанными. Доход злоумышленников составляет порой сотни миллионов долларов США.

По сообщению американской компании Symantec [8], мирового лидера по разработке программного обеспечения в области информационной безопасности и защиты информации, в 2017 г. 143 млн американских потребителей, ставших жертвами киберпреступности, потеряли 19,4 млрд долл. США.

В марте 2018 г. аналитики антивирусной компании McAfee подсчитали, что в 2017 г. мировой ущерб от киберпреступлений составил около 600 млрд долл. США, или 0,8 % от мирового ВВП, увеличившись примерно на 35 % по сравнению с оценкой за 2014 г. в 445 млрд долл. США [9].

Наиболее распространенные киберпреступления включают:

– заражение устройства вирусом или другая угроза безопасности (57 %);

– мошенничество с дебетовыми или кредитными картами (54 %);

– хищение информации и персональных данных пользователя (54 %);

– подверженность риску пароля учетной записи (40 %);

– несанкционированный доступ или взлом электронной почты или учетной записи в социальных сетях (40 %);

– совершение онлайн-покупки по мошеннической схеме (33 %);

– предоставление конфиденциальной (личной/финансовой) информации на мошеннический адрес электронной почты (34 %) [8].

Формат киберпреступлений трансформируется год от года. Первоначально с внедрением компьютерной техники и интернет-технологий появились вредоносные программы и вирусы-вымогатели. Постепенно с развитием хакерских методов шпионажа они трансформировались во взломы почтовых ящиков, затем основная угроза перешла в «темный» интернет и криптовалютную индустрию, а сейчас хакеры постепенно захватывают интернет вещей. Отчет Symantec 2018 Internet Security Threat Report [10] свидетельствует о 600 %-ном увеличении атак на этот сегмент.

По данным ежегодного отчета Hi-Tech Crime Trends 2018 международной компании Group-IB [11], специализирующейся на предотвращении кибератак, мошенничество с банковскими картами остается в числе наиболее опасных угроз для физических лиц: недостаточное распространение систем поведенческого анализа при проведении транзакций приводит не только к прямому ущербу, но и к росту бизнеса кардшопов. Ежемесячно в мире для продажи в кардшопах загружаются около 686 тыс. текстовых данных скомпрометированных банковских карт и 1,1 млн дампов[1]. Общий объем рынка кардинга по итогам второй половины 2017 г. – первой половины 2018 г. составил 663 млн долл. США.

Все больше компаний переносят важные данные и коммерческие приложения в облако, а значит, подобные сервисы становятся привлекательными для киберпреступников. Крупные провайдеры, давно работающие на этом рынке – Google, Amazon, IBM – обладают достаточными ресурсами и опытом, чтобы противостоять атакам. Небольшие региональные облачные сервисы остаются весьма уязвимыми. Согласно анализу экспертов из Risk Based Security [12], только за первую половину 2018 г. было украдено 6 млн записей с персональной информацией пользователей, произошло 2200 крупных взломов. Практически нет сомнений, что в 2019 г. могут повториться масштабные утечки данных, подобные провалу бюро кредитных историй Equifax, когда хакеры вынесли персональную информацию 143 млн клиентов.

Group-IB отмечает [11], что фокус перспективной разработки и инноваций в создании сложных вирусов, а также проведении многоступенчатых целевых атак сместился от финансово-мотивированных киберпреступников к проправительственным внедрениям в сети объектов критической инфраструктуры оборонного комплекса, энергетической промышленности, здравоохранения и транспортной системы с целью обеспечения долговременного присутствия, саботажа и шпионажа за компаниями. Преступники, атакующие объекты критической инфраструктуры, руководствуются, прежде всего, идеологическими и (реже) финансовыми мотивами, другие значимые цели кибератак – шпионаж и саботаж. Помимо получения информации, в цели злоумышленников входит максимальное закрепление, контроль инфраструктуры и каналов коммуникации. В топ-3 стран происхождения самых активных проправительственных хакерских групп входит Китай, Северная Корея и Иран. В 2018 г. была раскрыта новая хакерская группа – Silence. Помимо нее сегодня самыми опасными для банков во всем мире являются MoneyTaker, Lazarus и Cobalt.

Новое поле для деятельности киберпреступников появилось с развитием криптоиндустрии и фишинга[2]: около 56 % всех средств, украденных с ICO, были похищены с помощью фишинговых атак [11]. Аналитики Ernst & Young в декабре 2017 г. сделали неутеши-

[1] Дампом (от англ. *to dump* – сбрасывать) называется файл с полным или частичным содержимым памяти компьютера или базы данных в момент создания этого файла, т.е. снимок информации о состоянии компьютерной системы.

[2] Фишинг – один из видов интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам, паролям, данным лицевых счетов и банковских карт. Выделяют несколько основных видов фишинга: почтовый (рассылка различных электронных сообщений), онлайновый (копирование наиболее популярных интернет-ресурсов) и комбинированный.

тельный вывод: из привлеченных за два года в сфере ICO 3,7 млрд долл. США было украдено почти 400 млн долл. США [13]. Исследования показали, что хакеры не только ежемесячно похищали деньги на сумму около 1,5 млн долл. США, но также получали доступ к личным данным участников ICO, в том числе к их адресам, телефонным номерам и банковским сведениям. Это повлияло на ужесточение регулирования ICO во многих странах: Китай и Южная Корея запретили проводить первичное размещение токенов, а Япония, Канада, США и Австралия ввели новые правовые нормы.

С 2017 г. значительно возрос интерес хакеров к атакам с целью взлома криптобирж и криптоджекинга[3]. Ущерб от взлома 14 криптовалютных бирж составил более 882 млн долл. США. В середине сентября 2018 г. была ограблена японская криптовалютная биржа Zaif. Атакующие похитили средства в трех криптовалютах (Bitcoin, Bitcoin Cash и MonaCoin) на общую сумму 6,7 млрд иен (примерно 60 млн долл. США).

Компания Symantec в своем 23-м отчете об угрозах безопасности в интернете [10] также указывает на рост числа случаев киберпреступлений, связанных с использованием криптовалюты. Наиболее яркими примерами являются криптоджекинг и вымогательство.

Аналитики Symantec утверждают, что количество заражений с помощью криптоджекинга, обнаруженных на компьютерах, в 2017–2018 гг. увеличилось на 8500 %. После выхода ПО для скрытого майнинга Coinhive, появилось еще семь программ подобного типа. Эксперты прогнозируют, что крупнейшие майнеры в мире могут стать целью не только киберпреступников, но и прогосударственных атакующих групп. При определенной подготовке это может позволить им взять под контроль 51 % мощностей для майнинга и захватить управление криптовалютой. Сразу пять успешных «атак 51 %» было зафиксировано в первой половине 2018 г.: сумма прямого финансового ущерба составила от 0,55 млн до 18 млн долл. США [10].

За последние годы одной из самых серьезных угроз в киберпространстве стали вирусы-вымогатели. В 2017 г. количество их атак увеличилось на 2502 % [10]. При этом, по информации «Лаборатории Касперского», было обнаружено много модификаций новых и известных программ-вымогателей – более 96 000 по сравнению с 54 000 в 2016 г. [14]. Согласно отчету Verizon 2018 Data Breach Investigations Report [15], атаки вымогателей являются наиболее распространенным типом вредоносного ПО. Они были использованы в 39 % случаев взлома, что в два раза выше, чем в 2016 г. Более того, анализ Verizon показывает, что атаки теперь переходят в критически важные для бизнеса системы, шифруют файловые серверы или базы данных, наносят больший ущерб и требуют больше выкупа. Жертвами вымогателей стали государственные предприятия, частные компании, больницы и обычные пользователи. По подсчетам Carbon Black, в «темном» интернете сегодня выставлено на продажу 25 тыс. подобных программ. Причем, если недавно главной целью злоумышленников было оборудование с Windows, то теперь они переключились и на системы с Mac и Linux, а также взлом смартфонов.

По мнению экспертов, направление вирусов-вымогателей будет на подъеме и в 2019 г. Во-первых, уже сейчас преступники находят способы обойти или отменить резервное копирование взламываемой системы. Во-вторых, ничто не мешает им начать использовать технологии искусственного интеллекта и машинного обучения, чтобы делать атаки более персонализированными, точно знать, кого и когда можно взламывать в конкретной организации.

Благодаря новым технологиям прослеживается тенденция сокращения времени обнаружения киберугроз: медианное время обнаружения (Time to Detection, TTD) в ноябре 2015 г. составляло 39 ч, с ноября 2015 г. по октябрь 2016 г. – 14 ч, с ноября 2016 г. по октябрь 2017 г. – около 4,6 ч. Согласно данным Cisco 2018 Annual Cybersecurity Report [16], специалисты по защите, стремясь сократить время обнаружения злоумышленников, начинают все чаще делать ставку на автоматизацию (39 %), машинное самообучение (34 %) и искусственный интеллект (32 %). По другую сторону баррикад в ход идут облачные сервисы: преступникам удается избежать обнаружения с помощью шифрования, которое помогает скрыть активность потока команд и управления. В связи с этим, несмотря на достигнутые успехи, в мире с каждым годом растут расходы на обеспечение кибербезопасности.

Так, аналитики IDC прогнозируют [17], что глобальные расходы на аппаратное и программное обеспечение, а также сервисы, связанные с кибербезопасностью, в 2022 г. превысят 133,7 млрд долл. США. Хотя рост расходов в период с 2017 по 2022 г. замедлится, показатель CAGR[4] составит ощутимые 9,9 %. Как итог, результат 2022 г. на 45 % превысит достижение 2018 г., по итогам которого объем расходов составит 92,1 млрд долл. США. Крупнейшим инвестором в средства безопасности окажутся банки – их общие затраты вырастут с 10,5 млрд в 2018 г. до 16,0 млрд долл. США по итогам 2022 г. Следом разместятся дискретное производство (8,9 млрд долл. США) и центральные/местные органы власти (7,8 млрд долл. США). Наибольший рост расходов покажут телекоммуникации (13,1 % CAGR), центральные/местные органы власти (12,3 % CAGR) и сырьевая индустрия (11,8 % CAGR). Крупнейшим географическим рынком останутся США, которые в 2018 г. потратят на средства кибербезопасности 39,3 млрд долл. США, следом разместятся Великобритания (6,1 млрд долл. США) и Китай (5,6 млрд долл. США).

Между тем, в середине августа 2018 г. специалисты исследовательской компании Gartner заявили [18], что по итогам 2017 г. глобальные расходы на информационную безопасность (продукты и услуги) уже до-

[3] Криптоджекинг – использование мощностей компьютера для майнинга криптовалюты без ведома владельца машины. В основном предпочтение отдается анонимным криптовалютам, таким как Monero: во-первых, потому что она обеспечивает максимальный уровень анонимности для преступника, во-вторых, обычные процессоры, установленные на большинстве компьютеров, могут эффективно майнить эту монету.

[4] Совокупный темп годового прироста.

Таблица – Мировые расходы на кибербезопасность по сегментам в 2017–2019 гг., млн долл. США

Сегмент рынка / Год	2017	2018	2019
Безопасность приложений	2434	2742	3003
Безопасность облачных сервисов	185	304	459
Безопасность данных	2563	3063	3524
Управление идентификацией и доступом	8823	9768	10578
Защита ИК-инфраструктуры	12583	14106	15337
Интегрированное управление рисками	3949	4347	4712
Оборудование для обеспечения сетевой безопасности	10911	12427	13321
Другое программное обеспечение для обеспечения безопасности информации	1832	2079	2285
Услуги киберзащиты	52315	58920	64237
Программное обеспечение безопасности потребителей	5948	6395	6661
Всего:	101544	114152	124116

3. Национальные стратегии кибербезопасности

Возникновение нового вида преступности – организованной киберпреступности – заставляет экономических агентов и государство выделить основные задачи по предотвращению киберугроз в следующих направлениях: защита персональных данных человека; безопасность коммерческих информационных систем; безопасность информационных систем государственных структур; защита рабочей среды, технологий и инструментов [19, с. 12]. В связи с подобными масштабными задачами кибербезопасность все чаще рассматривается как стратегическая проблема государственной важности, затрагивающая все слои общества. Государственная политика кибербезопасности служит средством усиления безопасности и надежности информационных систем государства.

В течение 2011–2018 гг. практически все страны-члены Евросоюза опубликовали свои государственные стратегии кибербезопасности (или их новые редакции). Так, были утверждены Национальная стратегическая основа безопасности киберпространства Италии 2013 г., Стратегия кибербезопасности для Германии 2016 г., Национальная стратегия кибербезопасности Великобритании на 2016–2021 гг., Национальная стратегия кибербезопасности Швеции 2017 г. и т.д. [20]. Подобные стратегии имеют Австралия (2016), Индия (2013), Канада (2018), Китай (2016), Япония (2015) и др. В конце 2016 г. была утверждена новая Доктрина информационной безопасности Российской Федерации, в июне 2017 г. принята Концепция кибербезопасности «Киберщит Казахстана», а в октябре 2018 г. утверждена Стратегия кибербезопасности финансового сектора Республики Казахстан на 2018–2022 гг.

В сентябре 2018 г. Президентом США Д. Трампом подписана новая редакция Национальной стратегии кибербезопасности [21], которая ориентирована на обеспечение мира силой путем укрепления могущества и усиления роли США на международной арене.

Важным элементом политики по расширению своего влияния является продвижение новых технологий и предоставление консультаций по вопросам развертывания инфраструктуры, управления рисками, выработки политики и стандартов совместимости в интернете. При этом американские рынки под предлогом национальной безопасности закрываются для товаров и услуг, предоставляемых компаниями из «неблагонадежных» государств, к которым, по мнению США, относятся прежде всего Россия и Китай. Подобные шаги других стран – например, требование о хранении персональной информации на серверах внутри страны, – объявляются подрывающими конкурентоспособность американских компаний.

Предполагается расширение возможностей правоохранительных органов по сбору необходимых доказательств преступной деятельности и проведения оперативно-следственных в том числе и за пределами США в соответствии с принятым в 2018 г. «CLOUD Act»; теперь заключение соглашений и соответствующее уведомление государств о проведении следственных мероприятий на их территории больше не требуется. Несмотря на имеющиеся фундаментальные проблемы Европейской Конвенции по киберпреступлениям (Будапешт, 2001)[5], Администрация США и далее будет работать над расширением международного консенсуса в пользу Конвенции. Проект резолюции ООН «О сотрудничестве в сфере противодействия информационной преступности» (2017), предлагаемый Россией, не рассматривается даже с критических позиций.

[5] Россия не подписала Конвенцию из-за статьи 32, которая позволяет различным спецслужбам без официального уведомления получать трансграничный доступ к компьютерным данным, что несут угрозу безопасности и суверенитету страны. До сих пор не присоединились к Конвенции Беларусь, Бразилия, Индия, Казахстан, Китай и др.

4. Проблемы международного сотрудничества в сфере кибербезопасности

Для борьбы с киберпреступностью чрезвычайно важно международное сотрудничество, которое должно осуществляться вне политического контекста. К сожалению, текущие политические события очень сильно осложняют процесс совместной работы над расследованием и предотвращением киберугроз. Регулирование сферы киберпространства на международном уровне выбивается из существующей практики, камнем преткновения становится трансграничность киберпространства: любой конфликт неизбежно приобретает международное измерение и с высокой вероятностью затрагивает гражданскую инфраструктуру и третьих лиц. Государства не только используют технологии в целях разведки и военного превосходства, но и совершают противоправные действия, оценка которых неоднозначна с точки зрения применения международного права, поскольку механизм для этого до сих пор не выработан. Однако помимо технических, имеются также политические и юридические проблемы регулирования.

Во-первых, существует различное понимание кибербезопасности у «восточных» и «западных» государств, а также угроз, исходящих из киберпространства. Эти несоответствия препятствуют государственному диалогу о правилах и нормах ответственного поведения. Во-вторых, после пяти раундов работы Группы правительственных экспертов ООН в сфере информатизации и телекоммуникации в контексте международной безопасности (ГПЭ) наблюдается нежелание государств – членов группы продолжать дальнейшее сотрудничество. В-третьих, сегодня большинство ведущих государств уклоняются от выработки и подписания каких-либо юридически обязывающих соглашений по кибернормам, поскольку это введет за собой правовую ответственность за нарушение обязательств. Все это свидетельствует о том, что раскол между проамериканским и пророссийско-китайским видением будущего ИКТ-среды только нарастает.

Следует отметить, что в 2004–2015 гг. государства признали применимость существующего международного права и Устава ООН к киберпространству, выработали список норм и принципов ответственного поведения государств при использовании ИКТ, определили меры укрепления доверия и дальнейшего международного сотрудничества. Однако последний созыв ГПЭ в 2017 г. завершился неэффективно и поставил продолжение переговоров под вопрос, в том числе из-за позиции США и их сторонников, которые заявили, что данный формат исчерпал себя. Наиболее спорными стали вопросы применения права государства на самооборону в ответ на вредоносное использование ИКТ, а также применение международного гуманитарного права к киберпространству, что, по мнению некоторых участников группы, узаконило бы сценарий военных действий в контексте ИКТ. Свою роль сыграли и напряженные отношения между Россией и США, которые являются одними из постоянных участников ГПЭ. Как известно, американская сторона обвинила Россию во вмешательстве в американские президентские выборы 2016 г., а также в совершении кибератак и проведении информационных кампаний в социальных сетях [22].

Тем не менее, в Первом комитете Генеральной Ассамблеи ООН в начале ноября 2018 г. были одобрены проекты двух принципиально разных резолюций: спонсорами первого – «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности» (в поддержку высказалось 139 стран, против – 11) – выступили 36 государств, в том числе и США; 27 стран-спонсоров, включая Россию, Китай и других членов ШОС, а также несколько государств Африки и Латинской Америки представили свой проект – «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» (поддержана 109 голосами, против – 45, воздержались – 16). Кроме того, Третий комитет одобрил представленный второй группой и носящий технический характер проект резолюции «Противодействие использованию информационно-коммуникационных технологий в преступных целях» (в поддержку высказались 88 стран, против – 55, воздержались – 29).

Очевидно, что ни один из двух проектов резолюций не будет принят в исходном виде. Российское предложение несет в себе серьезную нагрузку в виде обновленного свода международных правил, норм и принципов ответственного поведения государств из 25 пунктов, который строится на идее суверенитета в киберпространстве. Против него активно выступают все западные страны. К тому же, российское предложение проигрывает в количестве соавторов, а количество оставшихся «влиятельных» неопределившихся стран уже не так велико, чтобы рассчитывать на значительное усиление поддержки. Американский проект выделяет важность добровольного характера норм и правил ответственного поведения государств и является более нейтральным по содержанию, однако предложения об обязательной публикации национальных позиций участников группы могут устроить не всех, в том числе Китай. Также предлагаемый принцип справедливого географического распределения и отсутствие условия достижения консенсуса по итогам работы лишает участников группы возможности «заблокировать» публикацию доклада, если результаты идут вразрез с их позициями.

Таким образом, на данный момент группы государств-единомышленников диаметрально противоположны в своем видении кибербезопасности и не готовы променять свою относительную свободу действий в киберпространстве ради всеобщей безопасности и стабильности.

5. Угрозы и вызовы кибербезопасности в Республике Беларусь

Что касается Беларуси, то в исследовании «Глобальный индекс кибербезопасности 2017» Международного союза электросвязи наша страна заняла 39-е место из 193 стран (в то время как Грузия – 8-е место, Россия – 10-е) [23]. Характерная черта Беларуси – инициативы по защите детей, включающие государственно-частное партнерство. Министерство образования совместно с мобильным оператором «МТС» реализовали программу по обучению детей безопасному пользованию интернетом. Обучение прошли уже около 6 тыс. детей. «Болевыми точками» Республики Беларусь являются

недостаток отраслевых центров кибербезопасности (CERT), отсутствие профессиональных стандартов в области кибербезопасности и механизмов стимулирования, не налаженное межведомственное сотрудничество, отсутствие стратегии по организации борьбы с преступлениями против информационной (или кибер-) безопасности.

В составе Министерства внутренних дел Республики Беларусь действует Управление по раскрытию преступлений в сфере высоких технологий (условное наименование «Управление «К»), отвечающее за организацию борьбы с преступлениями против информационной безопасности, или киберпреступлениями.

Следует отметить, что в белорусских документах вопросам кибербезопасности пока уделено явно недостаточное место. Например, в настоящее время в Беларуси вообще отсутствует определение кибербезопасности, в Концепции национальной безопасности Республики Беларусь 2010 г. используется более широкое понятие «информационная безопасность».

Среди задач формирования в Республике Беларусь цифровой экономики, перечисленных в Государственной программе развития цифровой экономики и информационного общества на 2016–2020 гг., борьба с киберпреступлениями и повышение кибербезопасности не значатся вообще. Указано лишь, что одним из направлений развития цифровой экономики является увеличение объема производства и безопасного потребления высокотехнологичных и наукоемких ИКТ товаров и услуг, а инфраструктура информатизации должна обеспечить безопасность информационных потоков. В документе даже не перечислены вызовы и угрозы кибербезопасности цифровой экономики в Республике Беларусь.

Между тем статистика свидетельствует, что состояние криминогенной обстановки в сфере высоких технологий постоянно ухудшается. Так, данные по 2017 г. в сравнении с 2012 г. свидетельствуют об увеличении (с 2040 до 3099, т.е. на 51,9 %) количества выявленных киберпреступлений [24].

При этом рост числа таких уголовно наказуемых деяний отмечается во всех регионах, наиболее значительный – в г. Минске (с 818 до 1 080, рост составил 32,0 %;), Брестской (с 260 до 343, на 31,9 %;), Гродненской (с 206 до 266, на 29,1 %;) и Минской (с 311 до 396, на 27,3 %;) областях.

Почти 3/4 преступлений (2318, или 74,8 %), выявленных в 2017 г. в сфере высоких технологий, относятся к хищениям путем использования компьютерной техники. Наблюдается рост числа выявленных фактов несанкционированного доступа к компьютерной информации (всего за год – с 258 до 462, или на 79,1 %).

Рост киберпреступности в Беларуси обусловлен рядом причин: интенсивно идет развитие и популяризация системы безналичных расчетов, появляется все больше устройств, осуществляющих финансовые транзакции. Значительно увеличилось число пользователей всевозможных электронных платежных систем. Наблюдается ежегодный прирост абонентов сотовой связи, держателей банковских платежных карт, интернет-пользователей. Шире стал сегмент рынка, который охватывает виртуальная территория. Уже не удивляет изобилие, разнообразие и доступность гаджетов, возможность подключения к интернету многих видов бытовой техники.

Республика Беларусь в сфере кибербезопасности испытывает следующие серьезные угрозы:

– низкая правовая грамотность населения и представителей бизнеса по вопросам кибербезопасности;

– нарушение субъектами информатизации и пользователями установленных технических стандартов и требований в сфере ИКТ, регламентов сбора, обработки, хранения и передачи информации в цифровой форме;

– технологические сбои и непреднамеренные ошибки персонала, которые оказывают негативное влияние на элементы ИК-инфраструктуры: программное обеспечение, информационные системы и сети и др.;

– действия международных преступных сообществ и отдельных граждан по осуществлению хищений в финансовой сфере, вредоносного воздействия с целью нарушений работы АСУ ТП промышленности, энергетики, связи, ИК-услуг;

– деятельность политических и экономических органов, террористических групп, разведывательных служб иностранных государств, направленная против интересов Республики Беларусь, путем оказания воздействия на ИК-инфраструктуру.

Недостаточная правовая грамотность населения и представителей бизнеса в вопросах информационной безопасности создают питательную среду для совершения правонарушений в информационной сфере, а низкая цифровая грамотность пользователей приводит к тому, что тысячи граждан Республики Беларусь становятся жертвами киберпреступников. Серьезным следствием того, что население Беларуси «отстранено» от проблем обеспечения кибербезопасности, также является недоверие граждан к онлайн-бизнесу, электронной торговле и другим важным составляющим цифровой экономики[6].

Между тем направление развития информационных технологий неразрывно связано с образованием граждан и представителей бизнеса, развитием человеческих ресурсов. Для этого необходимо формирование со школьной скамьи компьютерной грамотности и «цифровой гигиены», понимания элементов кибербезопасности.

К сожалению, большинство руководителей белорусских предприятий до сих пор воспринимают угрозы кибербезопасности в упрощенном виде: если на компанию осуществляется внешняя атака, с ней должны бороться внутренние системы информационной безопасности (пароли, ограничение доступа, файерволы, антивирусы и прочее). Мало кто осознает, что главной причиной всех утечек данных в мире, начиная с 2015 г., являются ошибки собственного персонала, самих пользователей, а не вредоносные программы как таковые. Человеческий фактор, согласно исследованиям, отвечает за 52 % всех взломов.

Эксперты уверены, что файерволы и антивирусные программы не имеют столь важного значения для защиты данных, как принято считать. Все потому, что подавляющее большинство цифровых угроз сегодня «клиен-

[6] По данным Министерства антимонопольного регулирования и торговли Республики Беларусь, в 2017 г. доля электронной торговли в общей розничной торговле составила всего 2,8 %.

тоориентированы», т.е. инициируются, умышленно или нет, самими пользователями. Основной риск заключается в наличии неисправного ПО и невнимании сотрудников, когда скачивается нечто, чего в корпоративной сети не должно быть. Произойти это может десятками разных способов, когда, например, пользователя заваливают письмами от имени финансовой организации, выпрашивая сведения для авторизации.

Более конкретные способы защиты от кибернетических угроз заключаются в применении на предприятиях стандартов мультифакторной идентификации пользователей. Исследование Verizon [15] утверждает, что 63 % всех подтвержденных утечек данных происходит из-за кражи или подбора пароля к системе безопасности. Поскольку больше половины подобных инцидентов случается по вине самих пользователей, необходимо свести влияние человеческого фактора к минимуму, внедрив технологии биометрической идентификации как механизм обеспечения кибербезопасности в цифровой экономике.

Биометрическая идентификация – это автоматизированный метод, с помощью которого регистрируют уникальные анатомо-физиологические особенности и поведенческие характеристики человека для дальнейшей идентификации его личности. Биометрические характеристики, в отличие от персонального идентификационного номера или пароля, не могут быть похищены, потеряны или забыты. Анатомические особенности, такие как папиллярный узор пальцев рук и складок ладони, рисунок радужной оболочки глаза, форма ушной раковины, структура ДНК, голосовые данные, индивидуальные запахи человека, походка, динамика подписи, клавиатурный почерк и другие считаются уникальными и неизменяемыми характеристиками человека на протяжении всей его жизни, тем самым обеспечивая высокую достоверность процесса идентификации. К перспективным биометрическим технологиям, находящимся в стадии разработки, относятся термограмма лица в инфракрасном диапазоне излучения, анализ структуры кожи и эпителия на пальцах на основе цифровой ультразвуковой информации (спектроскопия кожи), распознавание по расположению вен.

Большинство компаний по-прежнему использует одноуровневую идентификацию для доступа к ключевым приложениям и ресурсам системы, опасаясь, что более сложный алгоритм доступа будет мешать работе. Многие начали осознавать, что это ошибочный подход. Microsoft уже пытается интегрировать биометрические данные в процесс аутентификации в удобной для использования в коммерческих организациях форме. Не исключено, что в ближайшем будущем метод распознавания лиц, применяемый в смартфонах Apple и Samsung, будет использоваться и для доступа к корпоративным системам.

Издание PC уверено [25], что компании, которые начнут внедрять инструменты многоуровневой идентификации – биометрику, умные карты, даже просто отправку дополнительного пароля на личные телефоны сотрудников – существенно снизят риски безопасности своих данных.

6. Рекомендации по борьбе с киберпреступностью в Республике Беларусь

Несмотря на принимаемые меры, в Беларуси пока нет ясного понимания целей совершенствования существующей системы кибербезопасности и методов их достижения, а государственные чиновники часто оказываются не способны наладить конструктивный диалог с представителями экспертного сообщества. Речь идет не о принятии отдельных нормативно-правовых актов или политических решений по предотвращению потенциальных киберугроз, а о необходимости создания и функционирования постоянно обновляемой системы принятия системных мер в области планирования и реализации мероприятий по обеспечению кибербезопасности на всех уровнях ее функционирования.

В эпоху стремительного развития цифровых технологий первоочередными мерами по поддержанию экономической безопасности белорусского государства, предотвращению киберпреступлений должны стать:

– постоянно налаженный на международном уровне обмен информацией между государственными органами, общественными организациями и бизнес-сообществом об киберинцидентах, новых технологиях защиты, введение практики круглосуточного реагирования на инциденты в информационной среде для обнаружения, анализа и профилактики киберугроз;

– сотрудничество белорусских силовых структур с международными полицейскими организациями (Европол, Интерпол и т.д.) в совершенствовании процедур информирования, взаимной помощи и совместных действий по борьбе с киберпреступниками;

– повышение осведомленности ИК-специалистов, компаний и государственных органов в области кибербезопасности;

– организация мер по обеспечению защиты и безопасности объектов критической инфраструктуры;

– дальнейшая работа Национального банка Республики Беларусь по усилению безопасности банковской и платежных систем;

– регулярное освещение в СМИ успехов в борьбе с киберпреступниками, опубликование текстов решений и приговоров судов по преступлениям в киберсреде, комментирование действий правоохранительных органов по ликвидации организованной киберпреступности;

– беспрерывная работа над улучшением и совершенствованием системы кибербезопасности, установка систем обновлений информационной безопасности, регулярное сканирование уязвимостей сайтов и приложений, постоянная защита от вредоносных программ, использование антивирусных средств, персональных межсетевых экранов и систем обнаружения вторжений;

– формирование эффективной системы, нацеленной на предупреждение киберпреступлений, включая совершенствование уголовного законодательства, правоприменительной практики;

– принятие нормативных правовых актов, регулирующих функционирование киберпространства, использование криптовалют и технологий блокчейн;

– государственное финансирование программ по поиску киберпреступников и искоренению криминального бизнеса;

– доработка и реализация Государственной программы развития цифровой экономики и информационного общества на 2016–2020 гг., внедрение

технологии блокчейн в электронный гражданский документооборот;

– развитие рынка страхования киберрисков; предложение страховыми компаниями новых продуктов и программ по возмещению финансового и репутационного вреда от последствий утечки персональных данных или их незаконного использования.

Эксперты по кибербезопасности отмечают, что ключевую роль в борьбе с компьютерной преступностью играет изучение личности и характера преступников. Для этих целей недостаточно обладать техническим инструментарием – нужно знать опыт и историю преступников. Сам же формат борьбы тоже должен перейти на новый уровень: на данном этапе государства и частный сектор в основном занимают оборонительную позицию, в то время как в фокусе должна быть работа над проактивным поиском и обнаружением угроз.

В настоящее время по инициативе Оперативно-аналитического центра при Президенте Республики Беларусь разрабатывается Концепция информационной безопасности, в которую заложены революционные постулаты и выделена норма кибербезопасности. Предлагается решение задачи информационной безопасности через взаимодействие государства и бизнеса, в частности через проекты ГЧП с целью привлечения технологий, инвестпроектов. Приходится надеяться, что в готовящемся документе будут учтены все потенциальные негативные нюансы построения цифровой экономики.

Решение вопросов, связанных с повышением эффективности борьбы с киберпреступностью, сегодня крайне необходимо. Ведь задача, поставленная руководством Республики Беларусь по расширению государственными органами и банками электронных услуг населению, отнесена к категории стратегически важных для решения социально-экономических проблем, создания реального механизма противодействия коррупции. Вместе с тем чем шире будут использоваться ИКТ, тем больше будет рисков в их безопасном применении.

Заключение

Мы должны со всей ответственностью понять, что цифровая трансформация экономики – это не дело ближайших лет, этот процесс уже стремительно развивается, независимо от нашего желания. За внедрением цифровой экономики – будущее, и если мы хотим использовать этот шанс для повышения качества жизни, обеспечения конкурентоспособности страны и национальной безопасности, в течение 15–20 лет войти в группу лидирующих экономик мира, необходимо уже сегодня, немедленно предпринять решительные действия по минимизации грядущих рисков, в том числе в сфере кибербезопасности.

В связи с этим в Республике Беларусь существует необходимость принятия Концепции кибербезопасности Республики Беларусь, которая бы содержала нормы о государственной политике в сфере обеспечения информационной безопасности, мерах защиты информации, видах и источниках угроз в киберпространстве, первоочередных мероприятиях по обеспечению информационной безопасности и т.д.

Литература / References

[1] Касперская, Н. Цифровая экономика и риски цифровой колонизации: развернутые тезисы выступления на Парламентских слушаниях в Госдуме [Электронный ресурс] / Н. Касперская // Общественный совет гражданского общества. – Режим доступа: http://narodosnova.ru/2018/04/tsifrovaya-ekonomika-i-riski-tsifrovoj-kolonizatsii.html. – Дата доступа: 29.11.2018.

Kasperskaya, N. Tsifrovaya ekonomika i riski tsifrovoy kolonizatsii: razvernutyye tezisy vystupleniya na Parlamentskikh slushaniyakh v Gosdume [Electronic resource] / N. Kasperskaya // Obshchestvennyy sovet grazhdanskogo obshchestva. – Mode of access: http://narodosnova.ru/2018/04/tsifrovaya-ekonomika-i-riski-tsifrovoj-kolonizatsii.html. – Date of access: 29.11.2018.

[2] Номоконов, В.А. Киберпреступность как новая криминальная угроза / В.А. Номоконов, Т.Л. Тропина // Криминология: вчера, сегодня, завтра. – 2012. – № 1(24). – С. 45–55.

Nomokonov, V.A. Kiberprestupnost kak novaya kriminalnaya ugroza / V.A. Nomokonov, T.L. Tropina // Kriminologiya: vchera, segodnya, zavtra. – 2012. – № 1(24). – P. 45–55.

[3] Карпова, Д.Н. Киберпреступность: глобальная проблема и ее решение / Д.Н. Карпова // Власть. – 2014. – № 8. – С. 46–50.

Karpova, D.N. Kiberprestupnost: globalnaya problema i yeye resheniye / D.N. Karpova // Vlast. – 2014. – № 8. – P. 46–50.

[4] Об утверждении Концепции национальной безопасности Республики Беларусь [Электронный ресурс] : Указ Президента Республики Беларусь, 9 нояб. 2010 г., № 575; в ред. Указа Президента Респ. Беларусь от 24.01.2014 г. № 49 // Консультант Плюс.Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2018. – Дата доступа: 29.11.2018.

Ob utverzhdenii Kontseptsii natsionalnoy bezopasnosti Respubliki Belarus [Electronic resource] : Ukaz Prezidenta Respybliki Belarus, 9 noyab. 2010 g., № 575; v red. Ukaza Prezidenta Resp. Belarus' ot 24.01.2014 g. № 49 // Konsultant Plyus.Belarus / OOO «YurSpektr», Nats. tsentr pravovoy inform. Resp. Belarus. – Minsk, 2018. – Date of access: 29.11.2018.

[5] Зегжда, Д.П. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации / Д.П. Зегжда [и др.] // Вопросы кибербезопасности. – 2018. – № 2(26). – С. 2–15.

Zegzhda, D.P. Kiberbezopasnost progressivnykh proizvodstvennykh tekhnologiy v epokhu tsifrovoy transformatsii / D.P. Zegzhda [i dr.] // Voprosy kiberbezopasnosti. – 2018. – № 2(26). – P. 2–15.

[6] ISO/IEC 27032:2012. «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибер-

безопасности» [Электронный ресурс]. – Режим доступа: http://www.iso.org/iso/ru/catalogue_detail?csnumber=44375. – Дата доступа: 01.11.2018.

ISO/IEC 27032:2012. «Informatsionnyye tekhnologii. Metody obespecheniya bezopasnosti. Rukovodyashchiye ukazaniya po obespecheniyu kiberbezopasnosti» [Electronic resource]. – Rezhim dostuMode of accesspa: http://www.iso.org/iso/ru/catalogue_detail?csnumber=44375. – Date of access: 01.11.2018.

[7] Головенчик, Г.Г. Цифровая экономика как новый этап глобализации / Г.Г. Головенчик // Цифровая трансформация. – 2018. – № 1 (2). – С. 26–36.

Golovenchik, G.G. Tsifrovaya ekonomika kak novyy etap globalizatsii / G.G. Golovenchik // Tsifrovaya transformatsiya. – 2018. – № 1 (2). – P. 26–36.

[8] Norton Cyber Security Insights Report 2017. United States Results [Electronic resource] // Symantec. – Mode of access: https://www.symantec.com/content/dam/symantec/ docs/about/2017-ncsir-united-states-results-en.pdf. – Date of access: 29.11.2018.

[9] McAfee Labs Threats Report, March 2018 [Electronic resource] // McAfee. – Mode of access: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-mar-2018.pdf. – Date of access: 30.11.2018.

[10] Symantec 2018 Internet Security Threat Report [Electronic resource] // Symantec. – Mode of access: https://www.symantec.com/security-center/threat-report. – Date of access: 30.11.2018.

[11] Hi-Tech Crime Trends 2018. Отчет о тенденциях высокотехнологичных преступлений, октябрь 2018 года [Электронный ресурс] // Group-IB. – Режим доступа: https://www.group-ib.ru/resources/threat-research/2018-report.html. – Дата доступа: 30.11.2018.

Hi-Tech Crime Trends 2018. Otchet o tendentsiyakh vysokotekhnologichnykh prestupleniy, oktyabr 2018 goda [Electronic resource] // Group-IB. – Mode of access: https://www.group-ib.ru/resources/threat-research/2018-report.html. – Date of access: 30.11.2018.

[12] Over 2,200 Data Breaches Disclosed So Far In 2017, Exposing Over Six Billion Records [Electronic resource] // Risk Based Security. – Mode of access: https://www.riskbasedsecurity.com/2017/07/over-2200-data-breaches-disclosed-so-far-in-2017-exposing-over-six-billion-records/. – Date of access: 01.12.2018.

[13] EY research: initial coin offerings (ICOs), December 2017 [Electronic resource] // Ernst & Young. – Mode of access: https://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/%24File/ey-research-initial-coin-offerings-icos.pdf. – Date of access: 01.12.2018.

[14] Синицын, Ф. Kaspersky Security Bulletin: 2017. Сюжет года: шифровальщики атакуют / [Электронный ресурс] / Ф. Синицын // Лаборатория Касперского. – Режим доступа: https://securelist.ru/ksb-story-of-the-year-2017/88111/. – Дата доступа: 01.12.2018.

Sinitsyn, F. Kaspersky Security Bulletin: 2017. Syuzhet goda: shifroval'shchiki atakuyut / [Electronic resource] / F. Sinitsyn // Laboratoriya Kasperskogo. – Mode of access: https://securelist.ru/ksb-story-of-the-year-2017/88111/. – Date of access: 01.12.2018.

[15] Verizon 2018 Data Breach Investigations Report [Electronic resource] // Verizon. – Mode of access: https://enterprise.verizon.com/content/dam/resources/reports/2018/DBIR_2018_Report_execsummary.pdf. – Date of access: 02.12.2018.

[16] Cisco Annual Cybersecurity Report. Годовой отчет по кибербезопасности за 2018 год [Электронный ресурс] // Cisco. – Режим доступа: https://www.cisco.com/c/ru_ru/products/se curity/security-reports.html. – Дата доступа: 02.12.2018.

Cisco Annual Cybersecurity Report. Godovoy otchet po kiberbezopasnosti za 2018 god [Electronic resource] // Cisco. – Mode of access: https://www.cisco.com/c/ru_ru/products/security/security-reports.html. – Date of access: 02.12.2018.

[17] New IDC Spending Guide Forecasts Worldwide Spending on Security Solutions Will Reach $133.7 Billion in 2022 [Electronic resource] // IDC. – Mode of access: https://www.idc.com/getdoc.jsp?containerId=prUS44370418. – Date of access: 02.12.2018.

[18] Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019 [Electronic resource] // Gartner. – Mode of access: https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019. – Date of access: 02.12.2018.

[19] Удалов, Д.В. Угрозы и вызовы цифровой экономики / Д.В. Удалов // Экономическая безопасность и качество. – 2018. – № 1(30). – С. 12–18.

Udalov, D.V. Ugrozy i vyzovy tsifrovoy ekonomiki / D.V. Udalov // Ekonomicheskaya bezopasnost i kachestvo. – 2018. – № 1(30). – P. 12–18.

[20] National Cyber Security Strategies [Electronic resource] // ENISA. – Mode of access: https://www.enisa.europa.eu/topics/national-cyber-security-strategies. – Date of access: 03.12.2018.

[21] National Cyber Strategy of The United States of America 2018 [Electronic resource] // White House. – Mode of access: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. – Date of access: 03.12.2018.

[22] Стадник, И. Россия и США: два разных взгляда на кибербезопасность / И. Стадник // РСМД. – Режим доступа: http://russiancouncil.ru/analytics-and-comments/analytics/rossiya-i-ssha-dva-raznykh-vzglyada-na-kiberbezopasnost/. – Дата доступа: 03.12.2018.

Stadnik, I. Rossiya i SSHA: dva raznykh vzglyada na kiberbezopasnost / I. Stadnik // RSMD. – Mode of access: http://russiancouncil.ru/analytics-and-comments/analytics/rossiya-i-ssha-dva-raznykh-vzglyada-na-kiberbezopasnost/. – Date of access: 03.12.2018.

[23] Global Cybersecurity Index 2017 [Electronic resource] // ITU. – Mode of access: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCI-17Report.pdf. – Date of access: 03.12.2018.

[24] Статистические данные по киберпреступлениям за 2017 год [Электронный ресурс] // Министерство внутренних дел Республики Беларусь. – Режим доступа: http://mvd.gov.by/ru/main.aspx?guid=3311. – Дата доступа: 03.12.2018.

Statisticheskiye dannyye po kiberprestupleniyam za 2017 god [Electronic resource] // Ministerstvo vnutrennikh del Respubliki Belarus. – Mode of access: http://mvd.gov.by/ru/main.aspx?guid=3311. – Date of access: 03.12.2018.

[25] Rash, W. 5 IT Security Trends to Watch in 2018 / W. Rash [Electronic resource] // PC. – Mode of access: https://www.pcmag.com/article/358251/it-watch-security-in-2018. – Date of access: 03.12.2018.