Несмотря на имеющиеся практические руководства по виртуализации криминалистических образов, их реализация на практике достигается не всегда. Это зависит от вида виртуализируемой ОС (например, Windows, Linux, Android), емкости и доступности самого носителя, а также характеристик ранее используемого с ним устройства. Невзирая на имеющиеся проблемы, данный подход собирания цифровых доказательств можно признать перспективным для органов уголовного преследования и требующим дальнейшей разработки.

Список использованных источников

1. Уголовно-процессуальный кодекс Республики Беларусь [Электронный ресурс] : 16 июля 1999 г., № 295-З : в ред. Закона Респ. Беларусь от 20.07.2022 г. № 199-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

2. Association of chief police officers – Good Practice Guide for Digital Evidence (March 2012) [Electronic resourse]. – Mode of access: www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf. – Data of access: 08.12.2022.

3. National Institute of Standards and Technology – Guide to Integrating Forensic Techniques into Incident Response (August 2006) [Electronic resourse]. – Mode of access: tsapps.nist.gov/publication/get_pdf.cfm?pub_id=50875. – Data of access: 08.12.2022.

4. Методика исследования компьютерной информации : метод. рекомендации / Гос. ком. судеб. экспертиз Респ. Беларусь. – Минск, 2016.

5. Форум ИБ – Codeby.net: Виртуализация криминалистических образов в Windows [Электронный ресурс]. – Режим доступа: codeby.net/threads/ virtualizecija-kriminalisticheskix-obrazov-v-windows. 64120. – Дата доступа: 08.12.2022.

6. Security is FUN: Booting up evidence E01 image using free tools [Electronic resourse]. – Mode of access: www.securityisfun.net/2014/06/booting-up-evidence-e01-image-using.html. – Data of access: 08.12.2022.

УДК 343.98.06

Е.Н. Соболевский

НЕКОТОРЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ СЕТИ ИНТЕРНЕТ В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Новые тенденции в развитии информационных технологий создают новые риски для информационной безопасности любого государства. Цифровой мир стремительно расширяется, он становится мобильным,

управляет производством и технологическими процессами, охватывает всю среду обитания человека – от бытовых приборов до умных офисов и интеллектуального транспорта. Все больше информации передается через мобильные сервисы, ранее изолированные системы начинают взаимодействовать и обмениваться информацией, лавинообразно нарастает поток данных и объемы хранения. Внедрение новых парадигм организации распределенных крупномасштабных систем, таких как «Интернет вещей» (Internet of Things, IoT), приведет к новым рискам информационной безопасности, когда через сеть станут доступны почти все предметы, окружающие человека.

По мере развития технологий в окружающем человека мире появляется все больше устройств, находящихся под управлением микропроцессоров и программного обеспечения. С ростом числа внедрений решений на базе IoT, как считают эксперты, все больше атак будет направлено не только на программное, но и на аппаратное обеспечение (сетевые карты, USB-устройства), входящее в инфраструктуру «интеллектуального транспорта», «умных домов», автоматизированных систем управления производством и др.

Возможности коммуникаций, которые стали доступны государствам, юридическим и физическим лицам после возникновения глобальной компьютерной сети Интернет, привели к кардинальному преобразованию общества и его экономической реальности. Интернет сегодня – это среда, используемая для всевозможных форм взаимодействия всех субъектов экономики. Высокая степень необходимости интернета как в повседневных практиках общества, так и в деятельности государства и бизнес-сообщества, воздвигает его в ряд необходимых элементов социально-экономического развития общества. По состоянию на текущий год в мире насчитывается более 5 млрд пользователей сети Интернет – это 63 % от общего населения Земли. Об этом свидетельствуют данные отчета April Global Statshot report, подготовленного при участии We Are Social и Hootsuite.

Приоритетную важность представляет собой переход различных государственных отраслей экономики в цифровое пространство – электронное правительство. Предоставление цифровых услуг населению, создание государственных информационных систем и ресурсов, формирование межгосударственных каналов передачи данных сегодня представляют собой повсеместные практики.

На текущий момент 80 % организаций, прошедшие стадию цифровых преобразований (внедрение технологий «Индустрия 4.0»: промышленный Интернет вещей, большие данные, 3D-принтеры и др.), смогли существенно увеличить свою прибыль. Ежегодная прибыль компаний Samsung, LG, Huawei и др. оценивается в десятки млрд дол-

ларов США, что демонстрирует не только успешность цифровизации бизнес-процессов компаний, но и актуальность разрабатываемой ими продукции – технических средств и средств связи.

Сеть Интернет позволила сформировать новый рынок цифровых услуг и оказала значительное влияние на финансовое благосостояние стран. Так возникла экономика совместного использования (Sharing economy) – переход к платформенным решениям. Изначально базирующиеся на цифровых рынках платформы Google, Facebook (США), Amazon (США), Uber (США), Alibaba (Китай), Яндекс (Россия) являются гигантами цифрового мира и имеют исключительное конкурентное преимущество как на глобальном, так и на местном уровне.

В современных реалиях цифровая экономика стала мощным фундаментом развития государств: страны с более развитой цифровой экономикой получают большую долю своего ВВП за счет высокотехнологичных секторов. Предполагается, что к 2025 г. цифровая экономика может достичь показателя в 50 % глобального ВВП, а в развитых странах превысить его.

Киберугрозы сегодня нацелены на все области, использующие цифровые данные: здравоохранение, образование и науку, банковскую сферу, государственные органы, представителей бизнеса и многое другие. В большинстве случаев цель злоумышленников – хищение персональных данных: номера банковских счетов и кредитных карточек, паспортные данные, медицинские карты, данные об объектах интеллектуальной собственности, а также информация, относящаяся к государственной, коммерческой и военной тайне.

При рассмотрении области киберугроз на уровне государств можно отметить, что кибератакам подвержены как страны с высоким уровнем экономического развития (США, Китай, Канада и т.п.), так и с низким уровнем.

Наиболее актуальными угрозами можно считать:

социальную инженерию – это технологии манипулирования людьми в сети Интернет;

DDoS-атаки или отказ от обслуживания – это поток ложных запросов, блокирующих ресурс;

шифрование данных, которое в основном происходит при установке на компьютер программы-вымогателя (чаще всего через сеть Интернет при введении жертвы в заблуждение методами социальной инженерии). Данные программы блокируют доступ пользователей к их устройствам или блокируют доступ к файлам до тех пор, пока не будет выплачена денежная сумма или выкуп.

киберфизические атаки представляют собой взлом электрических сетей, транспортных систем, водоочистных сооружений и т. д.;

атаки на IoT (Интернет вещей) – это заражение устройства, подключенного к интернету;

киберпропаганду (дезинформация) и хактивизм (форма политической активности, при которой навыки компьютерного взлома широко используются против влиятельных коммерческих институтов и правительств, других целей).

Существующие и вновь возникающие угрозы кибербезопасности сегодня направлены на все структуры, имеющие выход в сеть Интернет: частные и государственные организации, производства, медицинские и образовательные учреждения, учреждения здравоохранения, финансовые и банковские структуры, а также многое другое.

Отсутствие необходимых навыков кибербезопасности активно влияет на ситуацию с киберпреступностью. В результате увеличения пропускной способности устройства, подключенные к Интернету вещей, стали более уязвимыми для кибератак. Многие устройства IoT не разработаны с учетом требований безопасности и могут иметь недостатки и уязвимости, которые легко используют злоумышленники. Если хакеры могут получить контроль над устройствами IoT в организации, они потенциально могут использовать их для доступа к остальной части ИТ-системы.

Таким образом, использование сети Интернет влечет за собой определенные риски, которые необходимо учитывать при проектировании, разработке и внедрении сетевых технологий. Полагается, что не стоит бояться использовать сеть Интернет, однако нужно использовать ее грамотно. Требуется вывести общество из состояния, вызванного опасностью использования сети, сформировать у граждан цифровую грамотность.

УДК 004.056.57; 004.89

М.Н. Сорокин, Д.С. Рябенко

ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РАЗВИТИИ АНАЛИТИКИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В ходе становления информационного общества процесс информатизации является одним из основных факторов его развития на современном этапе. Благодаря процессу информатизации субъект (человек, общество) включается в глобальное информационное пространство, становясь при этом его частью. Наиболее точно данный эффект можно сопоставить с нынешним состоянием технологии ис-