или ином сочетании в ОП, раскрывают потенциальные познавательные возможности ОП, которые реализуются в практической деятельности через разработанные в теории ОРД системы тактических приемов и комбинаций. Кроме того, особое значение процесс познания имеет при его научном исследовании. Проводя подобного рода исследования на монографическом уровне, ученые анализируют проблемные вопросы использования методов познания при выявлении оперативными сотрудниками латентных преступлений. На основании проводимых исследований вырабатываются новые научные рекомендации по реализации и использованию методов познания объективной действительности при осуществлении ОП, что позволяет повысить эффективность решения задач ОРД.

Исходя из вышеизложенного, можно сделать вывод, что процесс познания, происходящий при осуществлении ОП, является чувственно-рациональным. Используя научные и общие методы познания, оперативный сотрудник приобретает необходимые ему знания, которые позволяют решать оперативно-розыскные задачи по выявлению и раскрытию латентных преступлений.

УДК 004.5 + 004.7 + 334.024 + 338.2

Е.Н. Соболевский

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ

Новые возможности информационных технологий создают новые угрозы для информационной безопасности любой сферы общества. Цифровой мир стремительно расширяется, 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 нарастают поток данных и объемы их 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 практически 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 обеспечение, но и на аппаратное обеспечение (сетевые карты, USB-устройства), входящее в инфраструктуру интеллектуального транспорта, умных домов, автоматизированных систем управления производством.

Возможности, которые стали доступны с возникновением 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 потребности в интернете как в повседневных практиках общества, так и в деятельности государства и бизнес-сообщества выдвигает его в ряд необходимых элементов социально-экономического развития общества.

Сеть Интернет позволила сформировать новый рынок цифровых услуг и оказала значительное влияние на финансовое благосостояние стран.

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 другое. В большинстве случаев цель злоумышленников – хищение персональных данных (номера банковских счетов и банковских платежных карточек, паспортные данные, медицинские карты, данные об объектах интеллектуальной собственности), а также информации, относящейся к государственной, коммерческой и военной тайне.

Принято считать, что кибератакам подвержены все страны вне зависимости от уровня экономического развития.

На текущий момент основными видами атак, подпадающими под понятие киберугрозы, являются: киберфизические атаки, вредоносное программное обеспечение (включая программы-вымогатели, rootkit, backdoor, троянские программы, шпионские программы и т. д.), DDoS-атаки (потоки ложных запросов), ботнеты (компьютерные сети), социальная инженерия (в том числе фишинг) и т. д.

Данные инструменты применимы практически ко всем сферам деятельности государства, бизнесу и общественной жизни. Наиболее актуальными угрозами можно считать: социальную инженерию; DDoS-атаки или отказ от обслуживания; шифрование данных, которое в основном происходит при установке на компьютер программы-вымогателя; киберфизические атаки; атаки на IoT (интернет вещей); киберпропаганда (дезинформация) и иные.

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 знаний при разработке и внедрении сетевых технологий существенно влияет на ситуацию с киберпреступностью.

Данный период времени считается одним из наиболее тяжелых для экономики как на национальном, так и на мировом уровнях. Усложнившиеся санитарно-эпидемиологические условия позволили злоумышленникам использовать более изо-

щренные средства хищения данных. Так, киберпреступность выросла на 600 % из-за пандемии COVID-19. Наиболее важными проблемами в данной связи стали:

интерес пользователей сети Интернет, проявляемый к медицинским и фармакологическим данным, делает их мишенью для киберугроз;

сотрудники, работающие в удаленном режиме, являются основной мишенью для киберпреступников;

основной негативный аспект удаленной работы – увеличение количества утечек через различные сервисы;

отсутствие необходимых навыков кибербезопасности активно влияет на ситуацию с киберпреступностью;

в результате увеличения пропускной способности устройств, подключенных к устройствам IoT, они стали более уязвимыми для кибератак (многие устройства IoT разработаны без учета требований безопасности и могут иметь недостатки и уязвимости, которые легко использовать злоумышленникам; если хакеры могут получить контроль над устройствами IoT в организации, они потенциально могут использовать их для доступа к остальной части IT-системы).

При рассмотрении Республики Беларусь в контексте кибербезопасности можно утверждать, что проблемы внешнего мира (санитарно-эпидемиологические условия, незащищенность устройств IoT, недостаточная грамотность населения и специалистов в вопросах информационной безопасности и т. д.) также коснулись национального состояния дел. В рейтинге компании Comparitech (2020 г.) Беларусь вошла в 10 государств с низким уровнем кибербезопасности (наиболее проблемный аспект – финансовые вредоносные атаки).

Данные сведения демонстрируют необходимость ускорения развития области кибербезопасности в Республике Беларусь в соответствии с мировыми трендами и угрозами безопасности.

УДК 351.74:65

В.И. Стельмах

ТВЕРДЫЕ КОММУНАЛЬНЫЕ ОТХОДЫ КАК ФАКТОР ЭКОЛОГИЧЕСКОЙ И ЭНЕРГЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

Ежегодные объемы образования в Беларуси твердых коммунальных отходов (ТКО) оцениваются в пределах около 4 млн т, из которых только около 30 % перерабатываются и используются, а оставшиеся 70 % захораниваются. Захоронение ТКО представляет угрозу здоровью граждан, загрязняет поверхностные и подземные воды, леса и атмосферный воздух, иные компоненты и объекты окружающей среды, увеличивает выбросы парниковых газов. В соответствии с Концепцией национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575, образование больших объемов отходов при низкой степени их вторичного использования является одним из внутренних источников угроз экологической безопасности.

Полигоны, предназначенные для захоронения ТКО, занимают большие территории, в результате чего из хозяйственного использования исключаются значительные площади земельных ресурсов. Кроме того, эксплуатация и обустройство таких полигонов требуют значительных объемов финансовых ресурсов.

Особенно актуальна проблема образования и переработки ТКО для Минска, где образуется около 25 % отходов от всего их объема в стране. Все ТКО из столицы поступают и захораниваются на полигоне «Тростенецкий», который исчерпал свои возможности, и через несколько лет его планируется вывести из эксплуатации.

В то же время ТКО, являясь вторичными материальными ресурсами, постоянно возобновляемыми, могут эффективно перерабатываться и использоваться. Анализ мирового опыта использования ТКО показывает, что в таких странах, как Швейцария, Германия, Швеция, где утилизируется около 99 % бытовых отходов, почти половина после тщательной сортировки сжигается, в результате чего вырабатывается тепловая и электрическая энергия.

В последние годы в Беларуси предприняты значительные шаги по решению проблемы сбора и использования ТКО в качестве вторичных материальных ресурсов и топлива. В этих целях были разработаны и утверждены Правительством соответствующие нормативные правовые акты и планы. К их числу в первую очередь следует отнести такие документы, как Национальную стратегию по обращению с твердыми коммунальными отходами и вторичными материальными ресурсами в Республике Беларусь, Концепцию создания мощностей по производству альтернативного топлива из твердых коммунальных отходов и его использования и ряд других. Конкретные мероприятия по расширению использования ТКО в качестве альтернативного топлива нашли отражение в Государственных программах «Комфортное жилье и благоприятная среда», «Энергосбережение» на 2021–2025 годы и др.

Например, в числе основных целей Национальной стратегией по обращению с твердыми коммунальными отходами и вторичными материальными ресурсами в Республике Беларусь определены не только минимизация вредного воздействия ТКО на здоровье человека и окружающую среду, предотвращение их образования и максимально возможное вовлечение ТКО в хозяйственный оборот, но и энергетическое использование ТКО для получения тепловой и электрической энергии.

В указанных выше документах на основе анализа экономического и экологического значения энергетического использования ТКО определено, что наиболее оптимальным вариантом использования ТКО, обеспечивающим снижение негативного воздействия на окружающую среду и сокращение объемов захоронения ТКО, является энергетическое использование ТКО в виде пре-RDF-топлива и RDF-топлива. Пре-RDF-топливо производится из остатков в составе ТКО после извлечения мелкой фракции размером до 80 мм в виде органики и негорючих составляющих, а также извлечение наиболее ценных вторичных материальных ресурсов. RDF-топливо производится на основе переработки, измельчения следующих составляющих ТКО: резины, дерева (старая мебель, потерявшие потребительскую ценность строительные материалы из дерева, удаленные де-