Сделаем некоторые выводы. На современном этапе развития экономики наблюдается широкое проникновение ИКТ в социальные технологии. Система государственных электронных услуг представляет собой комплекс услуг, предоставляемых государственными органами в соответствии с их компетенциями по запросу граждан, организаций или других государственных органов с помощью использования ИКТ посредством транзакций обмена. Внедрение системы государственных электронных услуг изменяет принципы отношений между государством, гражданами и предпринимателями. Граждане и организации получают более широкий доступ к информации о государстве, административных процессах, организациях и действиях конкретных представителей государства. В результате смягчается проблема асимметрии информации между участниками процессов, растет открытость органов власти, создаются условия для более действенного общественного контроля над деятельностью отдельных государственных служащих. Использование ИКТ при оказании государственных электронных услуг уменьшает большую часть транзакционных издержек. В то же время порождаются новые виды затрат и издержек: идентификации пользователей, защиты имени, защиты личной информации, интерпретации информации, потери (искажения) информации и др. В целом система государственных электронных услуг повышает эффективность государственного и местного управления, укрепляет доверие между государством, публичными образованиями, гражданами и организациями предпринимателей, стимулирует развитие экономики страны. В то же время оказание государственных электронных услуг порождает новые социальные проблемы и технологические риски, для преодоления которых необходимы совместные целенаправленные усилия общества и государства.

УДК 340.113:004

О.А. Федоренко, младший научный сотрудник лаборатории по проблемам противодействия преступности Национальной академии внутренних дел (г. Киев, Украины)
Kseniya25@ukr.net

ИНТЕРНЕТ ВЕЩЕЙ КАК УЯЗВИМОЕ МЕСТО ДЛЯ ДЕСТРУКТИВНЫХ ДЕЙСТВИЙ КИБЕРПРЕСТУПНИКОВ

В настоящее время современный мир информационных технологий требует постоянного взаимодействия между своими компонентами. Однако люди имеют ограниченное время, внимание и точность. Все это означает, что человек – не лучший инструмент по сбору данных. В таких

условиях концепция коммуникации между устройствами предусматривает выполнение определенных действий вообще без вмешательства человека. Как следствие – вопрос разработки и внедрения технологий Интернет вещей активно обсуждается в Украине еще с конца XX в.

Понятие «Интернет вещей» (англ. Internet of things, IoT) рассматривается как сеть разнообразных объектов, увеличивается от промышленных устройств к потребительским товарам и услугам, которые могут обмениваться информацией и выполнять свои задачи.

Интернет вещей стремительно растет. По данным исследования консалтинговой компании, специализирующейся на рынках информационных технологий, Gartner по всему миру было 6,4 млрд подключенных вещей в 2016 г., что на 30 % выше, чем в 2015 г. В 2016 г. 5,5 млн новых вещей подключались к Интернету вещей ежедневно. С таким темпом, по прогнозу Gartner, к 2020 г. количество достигнет 20,8 млрд подключенных вещей.

Некоторые другие аналитические агентства выражают еще более оптимистичные прогнозы и предрекают 50 млрд подключенных устройств.

Высокий уровень неоднородности в сочетании с широкой гаммой систем IoT, как ожидается, увеличит число угроз безопасности владельцев устройств, которые все чаще используются для взаимодействия людей, машин и вещей в любой вариации. Традиционные меры обеспечения безопасности и конфиденциальности не могут быть применены к технологиям IoT, в частности, из-за их ограниченной вычислительной мощности.

Кроме того, большое количество подключенных устройств порождает проблему массовости. В то же время для достижения признания со стороны пользователей необходимо в обязательном порядке обеспечить соблюдение безопасности, конфиденциальность и модели доверия, которые подходят для контекста IoT. Для предотвращения несанкционированного доступа пользователей (т. е. людей и устройств) к системе должны использоваться механизмы аутентификации и авторизации, гарантированная безопасность, конфиденциальность и целостность персональных данных. По персональным данным пользователей и информации должны обеспечиваться защита и конфиденциальность, прежде всего потому, что устройства имеют к ней доступ и способны ей управлять (например, сведения о привычках пользователей).

Для Интернета вещей стоят сложные проблемы обеспечения безопасности по сравнению с теми, которые характерны для сетей связи. К ним добавляются возможные проблемы масштабируемости сети, вызванные мало предполагаемым объемом передачи данных от большого числа узлов, ненадежность программного обеспечения и т. п.

Широкое применение Интернета вещей – результат интеграции компьютерных технологий, технологий связи и различных областей промышленных отраслей. Кроме нарушения информационной безопасности традиционных сетей связи (в результате риска подслушивания, искажения информации, раскрытия информации) устройства и сети Интернета вещей сталкиваются с дополнительными проблемами безопасности на прикладном уровне – при использовании облачных вычислений, обработке информации, обеспечении прав на интеллектуальную собственность, защите приватности и т. д.

Угрозы для безопасности существующих сетей связи распространяются и на Интернет вещей, который построен на них. К ним относятся несанкционированный доступ, перехват данных пользователя, нарушения конфиденциальности, целостности информации, DoS-атаки, вирусы, эксплойты, сетевые черви и т. п. Кроме того, существуют межсетевые проблемы аутентификации, которые могут быть причиной DDoS и DoS-атак.

Распространение услуг IoT требует, чтобы были гарантированы безопасность и конфиденциальность. Таким образом, разрабатывая стратегию или политику по развертыванию систем Интернета вещей, следует учитывать сложность и относительную новизну этого явления, и вероятно возникновение непредвиденных социальных эффектов.

УДК 343.9

Э.Г. Хомяков, кандидат юридических наук, доцент кафедры криминалистики и судебных экспертиз Института права, социального управления и безопасности (ИПСУБ) Удмуртского государственного университета (УдГУ)
ed-18@yandex.ru

О СТАТИСТИЧЕСКОЙ ОТЧЕТНОСТИ, ДЕМОНСТРИРУЮЩЕЙ РЕЗУЛЬТАТЫ БОРЬБЫ С ПРЕСТУПНОСТЬЮ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Принятый в 1996 г. Уголовный кодекс (УК) Российской Федерации (РФ) в качестве одного из нововведений обозначил отдельную гл. 28 «Преступления в сфере компьютерной информации» (ст. 272–274). Революционная на тот период глава была введена как элемент противодействия новым видам преступлений, связанных с развитием информационных технологий.

Первые годы практической реализации положений данной главы, а именно раскрытия и расследования преступлений, предусмотренных ст. 272–274, позволили накопить необходимый опыт для борьбы с преступлениями «компьютерной направленности». Вместе с тем выявились и некоторые пробельные и проблемные моменты, не позволяющие говорить о наступательном противодействии указанному виду преступности со стороны различных правоохранительных структур, прежде всего МВД Российской Федерации. Возникли также проблемы в эффективном применении указанных статей УК РФ в различных субъектах Российской Федерации.

Накопленный опыт раскрытия и расследования преступлений в сфере компьютерной информации, а также тенденции в развитии информационных (компьютерных) технологий потребовали «ревизии» данной главы. В результате по истечении почти 15 лет с момента появления указанных видов преступлений был принят Федеральный закон от 7 декабря 2011 г. № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации», в соответствии с которым гл. 28 была подвергнута изменениям.

Еще одно изменение гл. 28 претерпела в 2017 г., когда с принятием Федерального закона от 26 июля 2017 г. № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» появилась новая ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

Основным субъектом расследования преступлений в сфере компьютерной информации согласно ст. 151 Уголовно-процессуального кодекса Российской Федерации являются следователи органов внутренних дел. Именно статистика МВД России дает наглядное представление о ситуации, возникшей на данном направлении борьбы с преступностью (см. табл. 4, 5).

Таблица 4

Количество преступлений в сфере компьютерной информации (гл. 28 УК РФ), зарегистрированных в Российской Федерации

Годы	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Количество преступлений	9 010	11 636	7 398	2 698	2 820	2 563	1 739	2 382	1 748	1 883	2 500