сурсы вышеуказанных недостатков лишены. Поэтому создание двух справочных информационно-поисковых систем («Пыльца древесных и кустарниковых растений, произрастающих на территории Республики Беларусь», «Пыльца травянистых растений, произрастающих на территории Республики Беларусь») даст возможность в значительной степени облегчить труд экспертов-биологов, связанный с необходимостью обработки больших объемов палинологической информации. Подготовленные информационно-поисковые системы будут включать в себя ключ для определения пыльцевых зерен растений, оптические микрофотографии пыльцы, а также другую техническую информацию и могут быть использованы как справочные и ориентировочные сведения в экспертных исследованиях.

Вышеуказанная работа позволит провести многоуровневое, комплексное исследование древесины и пыльцы, что, несомненно, представляет как научный, так и практический интерес. Внедрение новых подходов к экспертному исследованию данных объектов растительного происхождения в экспертную практику значительно расширит возможности судебной биологической экспертизы, повысит результативность, достоверность и научный уровень экспертных заключений, обоснованность выводов, улучшит общие показатели экспертной работы, а также обеспечит правоохранительные органы действенными методами получения новой доказательственной информации.

УДК 004:34

А.Н. Чаплинский

СОВРЕМЕННЫЕ РИСКИ И УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ

Информационные и коммуникационные технологии, стремительно развиваясь, прочно вошли в повседневную жизнь людей. С их развитием закономерно отмечается рост количества всевозможных киберугроз как отдельным государствам в целом, так и частным пользователям. На современном этапе развития общества проблемы кибербезопасности приобретают первостепенное значение.

По данным иностранных исследовательских центров в области кибербезопасности, ежегодный ущерб от деятельности киберпреступников будет составлять до 6 трлн долларов США (год назад 3 трлн долларов); в течение 2017–2021 гг. расходы на кибербезопасность составят около 1 трлн долларов США; количество подключенных к сети Интернет устройств к 2020 г. достигнет 12 млрд; к 2021 г. количество интернет-пользователей увеличится до 6 млрд (2015 г. – 2,4 млрд, 2017 г. – 3,8 млрд); ущерб от деятельности киберпреступников по распространению вредоносного программного обеспечения в 2017 г. составит 5 млрд долларов США (в 2015 г. – 325 млн долларов США).

В 2016 г. зарегистрировано более 90 млн кибератак, т. е. каждую минуту осуществлялось около 400 кибератак, причем около 70 % подобных атак остаются незамеченными для пользователя. Данная тенденция сохранится в обозримом будущем. И если ранее была распространена рассылка относительно безобидного спама в рекламных целях, то в последние годы отмечается рост числа вредоносных программ, имеющих целью незаконное завладение находящейся на устройствах пользователей компьютерной информацией. Все чаще киберпреступниками в качестве инструмента для осуществления своих противоправных посягательств используется массовая интернет-рассылка вредоносного программного обеспечения посредством электронной почты. Около 1 % электронных сообщений содержало вредоносное программное обеспечение – наивысший показатель за последние пять лет. Беспокойство вызывают хакерские атаки, имеющие целью шифрование находящейся на компьютерах пользователей информации с последующим вымогательством денежных средств за их расшифровку. И если в 2015 г. средняя сумма вымогаемой суммы составляла 294 доллара США, то в 2016 г. уже 1 077 долларов США.

Правоохранительные органы всего мира в борьбе с киберпреступностью сталкиваются с рядом проблем, главными из которых являются: анонимность в сети Интернет, шифрование злоумышленниками передаваемой информации и, как следствие, ограничение к ней доступа правоохранительных органов, а также ограниченная юрисдикция государств по борьбе с преступностью. Очевидно, что в существующих условиях акцент должен быть сделан на предотвращении кибератак и минимизации их негативных последствий.

Примечательна в этой связи история распространения вредоносной программы WannaCry, заразившей более 500 000 компьютеров по всему миру, в результате действия которой дезорганизована деятельность как частных компаний, так и госучреждений по всему миру. Прямые убытки компаний исчисляются миллиардами долларов США. Столь разрушительные последствия стали возможными вследствие игнорирования элементарных требований безопасности, в частности отсутствия обновлений установленных на компьютерах операционных систем. Так, массовая атака вирусом началась 12 мая 2017 г., в то время как еще в апреле 2017 г. компанией-производителем (Microsoft) выпущены обновления, устраняющие уязвимость в системе и таким образом предотвращающие заражение.

Республика Беларусь, являясь частью мирового информационного пространства, не может оставаться в стороне от происходящих глобальных информационных процессов. Отсутствие массовых кибератак в отношении Республики Беларусь не должно никого вводить в заблуждение и создавать иллюзию защищенности и является, скорее, результатом отсутствия интереса со стороны злоумышленников. Не в полной мере понимание на государственном уровне киберугроз и проблем, связанных с расследованием киберпреступлений, может негативно сказаться на состоянии информационной безопасности Республики Беларусь. Повсеместное использование в работе госучреждений устаревшего программного обеспечения (WindowsXP не поддерживается Microsoft с 8 апреля 2014 г.) наряду с отсутствием в достаточном количестве квалифицированных специалистов в области информационной безопасности в долгосрочной перспективе могут привести к негативным последствиям. В то же время хакерские атаки в отношении отдельных государств (вмешательство в избирательный процесс в США,

массовые сообщения о ложном минировании на территории Российской Федерации) неизбежно будут способствовать выработке в указанных государствах мер по борьбе с ними на государственном уровне.

Любопытен в этой связи рейтинг уровня кибербезопасности, представленный Международным союзом электросвязи, в котором Республика Беларусь занимает общее 39-е место (3-е среди стран СНГ) среди 193 стран-участниц. При составлении рейтинга эксперты принимали во внимание пять критериев: наличие правовых систем и структур, занимающихся вопросами кибербезопасности и киберпреступлений; технические возможности в области кибербезопасности; существование институтов координации политики и стратегий развития кибербезопасности на государственном уровне; наличие научно-исследовательских, образовательных и подготовительных программ, а также сертифицированных специалистов и госучреждений, способствующих наращиванию потенциала в сфере информационной безопасности; наличие партнерств, механизмов сотрудничества и систем обмена информацией. В проведенном исследовании внимание вызывает довольно низкий (0,33) индекс уровня наличия в Республике Беларусь институтов по координации политики и стратегий развития кибербезопасности на государственном уровне (для сравнения Грузия – 0,82, Россия – 0,85). Очевидно, что для более эффективной борьбы с киберпреступностью, нейтрализации возникающих угроз необходимо проведение в Республике Беларусь единой согласованной политики в области кибербезопасности.

Планируемое введение в Республике Беларусь с 1 января 2019 г. ID-карт взамен паспортов несомненно является важным шагом на пути построения в стране информационного общества, однако актуальным остается вопрос о защите содержащихся в них данных от несанкционированного доступа к ним злоумышленников. Введение указанных карт неизбежно спровоцирует активность хакеров по поиску уязвимостей в имеющихся системах безопасности. В качестве примера можно привести блокировку правительством Эстонии более 760 тыс. национальных ID-карт (население Эстонии составляет 1,3 млн человек) в связи с их уязвимостью и опасением использования злоумышленниками содержащихся в них данных.

Республика Беларусь столкнется с теми же проблемами в области информационной безопасности, что и мировое сообщество. Существенным шагом на пути минимизации негативных последствий от деятельности киберпреступников будет выработка единой государственной политики в области кибербезопасности, направленной на предотвращение и минимизацию негативных последствий киберпреступлений, эффективную деятельность правоохранительных органов по раскрытию и расследованию компьютерных преступлений.

УДК 343.98

В.А. Чванкин

ОСОБЕННОСТИ УСТАНОВЛЕНИЯ МЕСТА СТОЛКНОВЕНИЯ (НАЕЗДА) ТРАНСПОРТНЫХ СРЕДСТВ

При осмотре места дорожно-транспортного происшествия и проведении диагностических транспортно-трасологические экспертиз и исследований в рассматриваемом случае устанавливают место столкновения (наезда), определяют взаимное расположение транспортных средств в момент происшествия, распределение удара при столкновении, перемещение транспортных средств после него, взаимное положение транспортного средства и пешехода в момент наезда и т. д.

Установление места столкновения (наезда) транспортных средств является важным при определении механизма следообразования. Следы на месте дорожно-транспортного происшествия разнообразны и могут быть сгруппированы следующим образом: следы колес транспортных средств; следы повреждений на транспортных средствах; предметы и вещества, отделившиеся от транспортных средств в момент происшествия (различные детали, осколки стекла, пятна жидкостей, осыпь грязи, частицы краски и т. д.); положение транспортных средств на дороге; следы потерпевших (расположение деталей одежды, вещей, пятна крови и т. д.).

Наиболее точно определить место столкновения можно по следам колес. Так, в момент столкновения одного транспортного средства с другим, обладающим значительной массой, или с неподвижной преградой (например, стеной, столбом) происходит мгновенное гашение скорости, а за счет инерционного вращения колес образуются следы, похожие на следы буксования на месте (если сохраняется контакт колес с дорожным полотном).

В результате столкновения под действием внешних сил направление движения транспортного средства часто отклоняется от первоначального.

Появляются следы бокового скольжения или следы колес, заблокированных в момент удара. Начало этих следов и будет являться местом столкновения транспортных средств.

Если столкновение транспортного средства произошло с объектом, имеющим незначительную массу (например, наезд грузового автомобиля на велосипедиста, пешехода и т. д.), то место столкновения может не найти своего отражения в следах колес, поскольку транспортное средство продолжает движение и, как правило, не меняет направления. В этом случае происходит разрушение хрупких деталей (фар, подфарников, лобового стекла), которые осыпаются на дорогу по ходу движения, однако концентрируются в своей основной массе в месте столкновения.

Если скорость одного из столкнувшихся автотранспортных средств больше, то оно, продолжая двигаться в прежнем направлении, отбрасывает, поднимет или увлекает за собой объект столкновения. Определить точно место столкновения в этом случае затруднительно, поэтому здесь необходимо изучить дополнительные следы (осколки стекла, следы волочения и т. д.).

При столкновении тяжелого автотранспортного средства с более легкими по весу о месте столкновения могут свидетельствовать следы пробуксовки колес, а, также начало следов скольжения от деформированных деталей нижней части более легкого транспортного средства.