разработки, распространения, использования и согласно уголовному законодательству Республики Беларусь является уголовно наказуемым деянием независимо от наступивших последствий. Однако количество преступлений, совершенных с использованием вредоносного программного обеспечения в общем числе преступлений в сфере противодействия киберпреступности невелико. Связано это в первую очередь с трудоемкостью изготовления качественного вредоносного программного обеспечения, а также с высоким уровнем латентности данного вида преступлений. Помимо этого, в настоящее время в процедуре проведения проверки, проводимой по сообщениям и заявлениям о преступлениях и уголовным делам, расследуемым по признакам состава преступлений, предусмотренных ст. 212 и гл. 31 Уголовного кодекса Республики Беларусь, совершение которых сопряжено с использованием вредоносного программного обеспечения, имеются отдельные правовые и процессуальные проблемы.

Латентность данного вида преступлений обусловлена в первую очередь неочевидностью наступления последствий в результате совершения преступлений с использованием вредоносного программного обеспечения. Чаще всего пострадавшие не осознают происходящего заражения устройств и утечки данных, а последующее использование похищенных данных часто не позволяет связать его с предшествующим хищением данных. Таким образом, совершенное преступление остается безнаказанным и при этом влияет на формирование волн новых преступлений других видов (мошенничеств, хищений денежных средств путем модификации компьютерной информации, вымогательств и др.). Ввиду большого количества информационных систем потенциально подверженных угрозам со стороны злоумышленника, использующего вредоносное программное обеспечение, находящихся во владении частных лиц и организаций, необходимо осуществление дополнительного контроля за соблюдением организациями, работающими с персональными данными, реквизитами банковских платежных карточек и счетов и иными критически важными данными, Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» и приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 195 «О технической и криптографической защите персональных данных».

Второй и наиболее важный проблемный вопрос касается процесса проведения исследований для выявления вредоносного программного обеспечения. Современная практика сложилась таким образом, что оперативный сотрудник или следователь при выбытии на место происшествия по сообщению или заявлению о преступлении производит

осмотр места происшествия и в случае выявления достаточных данных о заражении устройства осуществляет изъятие накопителей информации устройства и в последующем направление их в Государственный комитет судебных экспертиз для проведения компьютерно-технической экспертизы. При этом заключение эксперта не позволяет дать ответ на вопрос о наличии или отсутствии вредоносного программного обеспечения. Экспертиза предоставляет лишь информацию о том, определяется ли тот или иной файл, хранящийся на исследуемом объекте антивирусным программным средством как вредоносное программное обеспечение. Получение данной информации не требует специальных познаний, и она может быть получена в ходе проведения осмотра компьютерной информации. Ввиду чего полноценное исследование вредоносного программного обеспечения не производится. К тому же отсутствие программы в базе данных вирусных сигнатур может привести к отрицательному ответу при даче оценки программному продукту как вредоносному, что в последующем приведет к принятию незаконного решения по материалу проверки или уголовному делу. При проведении полного исследования вредоносного программного обеспечения, с процессом изучения его возможностей, возможно установление принципа работы исследуемого программного продукта, способа внедрения, результата работы. В случае использования программного средства с целью хищения данных возможно установление данных об узле получателя данных. Вся эта информация окажет существенную помощь в раскрытии подобного вида преступлений. Следовательно, необходимо совершенствование системы экспертного исследования вредоносного программного средства.

УДК 343.985

А.А. Петрович, Д.Н. Лахтиков

ТЕХНОЛОГИЯ BIG DATA И СОВРЕМЕННЫЕ НАПРАВЛЕНИЯ ЕЕ ПРИМЕНЕНИЯ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

За последние несколько десятков лет объемы цифровых данных в мировой цифровой сфере растут в геометрической прогрессии. Сегодня количество информации, хранящейся на устройствах пользователей, серверах различных ресурсов и иных материальных носителях цифровой информации исчисляется в зеттабайтах. Это связано с неуклонно растущей ролью сети Интернет и цифрового пространства в

повседневной жизни современного человека, повсеместным внедрением облачных технологий, подразумевающих распределенное хранение данных и осуществление удаленного доступа к ним. Это обусловлено также постоянным совершенствованием технологий удаленной передачи данных и в целом развития сферы информатизации, порождающей новые виды цифровой информации, объем и разнообразие которых создают определенные сложности их обработки. Все эти факторы привели к появлению такого явления, как большие данные.

Термин «большие данные» до настоящего времени окончательно не сформировался в научной литературе. Его понимание лежит в области возникших на современном этапе развития проблем, связанных с обработкой информации. Сегодня принято определять термин «большие данные» исходя из основных характеристик цифровых данных:

большого объема;

разнообразия данных;

высокой скорости их изменения.

Однако такой подход является отчасти не полным и в большей степени унифицированным для понимания. Технология «Большие данные» имеет большое разнообразие вариантов применения, реализации и решаемых задач. Однако все варианты реализации включают в себя помимо самих данных и их характеристик еще два ключевых аспекта: технологии хранения данных и их анализа. В целом все указанные аспекты являются взаимосвязанными элементами технологии и напрямую влияют на ее возможности и эффективность.

К технологиям анализа следует отнести большой спектр технологий осуществления автоматизированной обработки данных. Основными перспективными направлениями в данной сфере являются: машинное обучение, статистический анализ и поиск аномалий.

Исходя из вышеназванных аспектов технологии «Большие данные», необходимо сделать вывод, что под данным термином следует понимать взаимосвязанную систему технологий хранения, структурирования и анализа большего объема цифровых данных, направленную на получение определенного результата.

К преимуществам технологии «Большие данные» относится возможность решения разнообразных задач анализа данных, обширный сектор сбора информации, относительная автономность и высокая скорость обработки данных. К недостаткам рассматриваемой технологии можно отнести высокую стоимость необходимого оборудования, а также необходимость в высококвалифицированном персонале обслуживания.

Сфера применения технологии «Большие данные» весьма разнообразна с учетом постоянно развивающего информационного простран-

ства. Рассматриваемая технология используется в медицине, генетике, метеорологии и иных направлениях, в том числе и в сфере правоохранительной деятельности.

Растущее внедрение информационных технологий во все сферы жизни также способствовало появлению различных схем совершения преступлений, с использованием так называемых фишинговых ссылок. Данные преступления чаще всего совершаются с использованием созданных злоумышленником поддельных интернет-страниц проверенных сервисов, внешне неотличимых от официальных ресурсов. В настоящее время такое направление особенно актуально ввиду невозможности постоянного мониторинга сети Интернет с целью выявления поддельных интернет-ресурсов и их оперативного блокирования с целью пресечения совершения преступлений в отношении граждан. Возможности технологии «Большие данные» с применением машинного обучения позволяют осуществлять постоянный мониторинг сети Интернет на предмет выявления поддельных ресурсов и подготовку оперативного решения о принятии мер по блокировке указанного ресурса. В перспективе имеется возможность автоматизации данного процесса от момента сбора информации до блокировки ресурса. Помимо этого, такое направление применения технологии «Большие данные» дает возможность осуществления операций мониторинга сети Интернет на предмет содержания ресурсами деструктивной информации, запрещенной законодательными актами государства к распространению, и принятия дальнейших решений в отношении указанного ресурса.

Учитывая, что в современной жизни каждый человек оставляет множество следов своего присутствия в сети Интернет, а объем и разнообразие подлежащих к анализу данных для выявления этих следов невообразимо огромны, методы ручного сбора информации о лице в интернете становятся слишком продолжительными. Существующие же технические решения не позволяют осуществить достаточно полный и глубокий анализ информации о лице. В связи с этими трудностями применение технологии «Большие данные» приобретает актуальность и в данной сфере и позволит деанонимизировать лицо, совершившее преступление.

Одним из наиболее значимых направлений правоохранительной деятельности является профилактика преступлений и правонарушений. Данное направление неразрывно связано с анализом и прогнозированием криминогенной обстановки. Работа по формированию эффективной организации деятельности органов внутренних дел на территории обслуживания с учетом криминогенной обстановки является одним из важнейших критериев, способствующих снижению уровня преступности в любом государстве. Постоянные процессы урбаниза-

ции и изменения обстановки в зависимости от огромного множества факторов, а также отсутствие возможности ее глобального отслеживания в режиме реального времени не позволяет эффективно принимать меры контроля оперативной обстановки на обслуживаемой территории. При этом при проведении анализа оперативной обстановки не всегда в полной мере возможно охватить все факторы ее формирования и изменения. Часто не учитываются социальные процессы в обществе, современные тенденции и экономическое состояние определенной территории. Технология «Большие данные», в зависимости от ее реализации, способна в режиме реального времени собирать и анализировать информацию о текущей обстановке на территории обслуживания органа внутренних дел и подготавливать оперативные прогнозы изменения криминогенной обстановки.

Таким образом, основным преимуществом использования рассматриваемой технологии в правоохранительной деятельности является формирование оперативного прогнозирования, способного оказать помощь сотрудникам органов внутренних дел в реагировании на формирующиеся изменения, касающиеся предупреждения, выявления и пресечения преступлений.

УДК 343.3

В.И. Пикта

НЕКОТОРЫЕ АСПЕКТЫ РАСПРОСТРАНЕНИЯ ПРОГРАММ-ВЫМОГАТЕЛЕЙ

Обеспечение защищенности информационных систем является одним из самых важных аспектов обеспечения информационной и национальной безопасности. Информация, в нынешних реалиях, является самым ценным объектом, который требует особого режима защиты. В таких условиях широкое распространение информации как ресурса послужило появлению вредоносного программного обеспечения, основной целью которого является компрометация информации и информационных систем.

Вредоносное программное обеспечение – это любое программное обеспечение, которое негативным образом влияет на работу персонального компьютера или радиоэлектронного устройства. Вредоносное программное обеспечение может быть представлено в виде всплывающего окна, которое не позволяет пользователю получить доступ к основному функционалу интернет-ресурса или к программному обеспечению, копирующему финансовую информацию с компьютера жертвы.

Согласно исследованиям «Лаборатории Касперского» в последние годы число новых семейств и разновидностей вредоносного программного обеспечения стремительно растет. «Лаборатория Касперского» ежедневно выявляет около 325 000 уникальных образцов вредоносных программ. Под угрозой находятся как домашние пользователи, так и крупные компании, банки, критическая инфраструктура, государственные организации, промышленные предприятия, использующие автоматизированные системы управления технологическими процессами.

Среди огромного ландшафта угроз в сфере распространения вредоносного программного обеспечения одним из лидеров выступают программы-вымогатели (шифровальщики). Данная угроза свойственна всем сферам функционирования информационных систем государственного и частного сектора. По статистическим сведениям, за 2021 г. мировой ущерб от распространения программ-вымогателей составляет около 20 млрд долл. США в связи с выплатой выкупов вымогателям и простоями.

Программа-вымогатель (от англ. ransomware – компиляция слов ransom – выкуп и software – программное обеспечение) является разновидностью вредоносного программного обеспечения, предназначенного для блокирования доступа к компьютерным системам или предотвращения считывания компьютерной информации (преимущественно с использованием методов шифрования), после чего от жертвы за дешифрование информации требуется выплатить денежные средства.

В научной литературе программы-вымогатели определяются как тип вредоносного программного обеспечения, которое поражает компьютерные системы, ограничивая доступ пользователей к данным, хранящимся в скомпрометированных системах. Восстановление измененной информации является трудоемким процессом, и многие жертвы выплачивают выкуп в целях получения ключей дешифрования. Однако выплата выкупа не гарантирует, что файлы будут дешифрованы или программа-вымогатель будет отключена или удалена для предотвращения повторения заражения информационных систем в будущем.

Угрозы, исходящие от программ-вымогателей, зависят от типа вируса, вследствие чего представляется возможным выделить две основные категории указанных программ: программы-блокировщики и программы-шифровальщики.

Программа-блокировщик – тип программ-вымогателей, предназначение которых блокировать работу персонального компьютера или мобильного устройства, с целью последующего требования выкупа. В отличие от программ-шифровальщиков, блокировщик не шифрует компьютерную информацию, а блокирует доступ к основному функционалу компьютерной системы. Предметом посягательства данного ви-