республики создавались дивизионы (моторизованные взводы) милиции. Эта мера позволила лучше оснастить их транспортом и средствами связи, улучшить служебную подготовку и воспитательную работу среди личного состава, способствовала повышению эффективности охраны общественного порядка. Существенным моментом в организации охраны общественного порядка стало принятие 20 июля 1974 г. нового Устава патрульно-постовой службы милиции, которым руководствовались сотрудники этих подразделений.

В независимой Республике Беларусь вопросам охраны правопорядка и профилактике также уделялось значительное внимание. 22 июня 1992 г. в органах внутренних дел были созданы отделы охраны правопорядка и профилактики. В результате реорганизации центрального аппарата МВД Республики Беларусь 29 января 2001 г. было создано Главное управление охраны правопорядка и профилактики милиции общественной безопасности. В начале 2004 г. оно было преобразовано в Главное управление милиции общественной безопасности и специальной милиции МВД Республики Беларусь. В 2008 г. вновь воссоздано Главное управление охраны правопорядка и профилактики милиции общественной безопасности МВД Республики Беларусь.

Таким образом, становление и деятельность подразделений охраны правопорядка и профилактики милиции общественной безопасности МВД Республики Беларусь связаны со следующими основными этапами в истории органов внутренних дел новейшего времени:

29 сентября 1920 г. – принятие приказа о формировании особого летучего отряда (ныне – День патрульно-постовой службы милиции);

17 ноября 1923 г. – принятие Инструкции участковому надзирателю (День образования службы участковых инспекторов милиции);

19 июня 1935 г. – принятие постановления «О ликвидации детской беспризорности и безнадзорности» (День образования инспекций по делам несовершеннолетних);

10 марта 1969 г. – в МВД БССР создано Управление административной службы милиции;

16 июня 1969 г. – издан приказ «Об объявлении штатов органов МВД БССР»;

30 декабря 1970 г. – издан приказ «Об утверждении Положения об Управлении административной службы милиции МВД БССР»;

22 июня 1992 г. – в органах внутренних дел Республики Беларусь созданы отделы охраны правопорядка и профилактики.

УДК 341.4

О.И. Левшук

ПРАВООХРАНИТЕЛЬНЫЙ ОПЫТ ПРОТИВОДЕЙСТВИЯ КИБЕРАТАКАМ

Киберпространство – важнейшая сфера боевых действий, способная оказать разрушительное воздействие на различные сферы: землю, воздух, море, космос и др. Многие государства вкладывают значительные суммы денег в обеспечение кибербезопасности, а именно для защиты компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных от атак злоумышленников.

Сокрушительные кибератаки исходят от китайских хакеров, которые на протяжении последних десяти лет активно атакуют объекты интеллектуальной собственности. В 2012 г. хакерскому нападению подверглась BAE Systems, в результате чего были похищены сведения о штурмовиках F-35, а в 2014 г. была взломана компьютерная сеть US Steel Corp. В 2015 г. были похищены терабайты секретных данных у предприятий оборонного комплекса США и взломана база данных управления кадров правительства США. В 2018 г. китайскими злоумышленниками похищены у поставщика Военно-морских сил США 614 гигабайт данных, в мае 2019 г. выявлен факт проникновения в компьютеры Агентства национальной безопасности США. Ответной реакцией на кибератаки стало усиление киберподразделений США, подготовка персонала посредством компьютерных полигонов с использованием облачных технологий.

По мнению многих исследователей, одной из основных причин кибератак является низкий уровень в компьютерной грамотности. Многие пользователи сети Интернет стали жертвами кибермошенников, последние смогли взломать программные продукты Apple (IOS), Microsoft (Visual Studio). Вредоносные программы проникают в компьютеры не только организаций государственной и частной форм собственности, но и физических лиц.

Активность киберпреступников и результативность их противоправной деятельности обусловлены нехваткой специалистов в области безопасности киберпространства. Решение такой проблемы многие американские компании видят в создании в иных странах своих офисов, для работы в которых приглашаются иностранные киберспециалисты. Например, в Норвегии, Дании, Швеции, Финляндии, Ирландии организовано обучение – функционируют учебные заведения для подготовки специалистов в сфере технологий, проектирования, математики с акцентированием внимания на компьютерную безопасность.

Правоохранительные органы и специальные службы Великобритании столкнулись с аналогичной проблемой, причем спрос на специалистов в компьютерной области значительно превышает предложение. Ситуация осложнена низким уровнем зарплаты и длительностью процесса проверки в государственных структурах, чем в частном секторе. Такая ситуация может быть разрешена путем повышения зарплаты, обеспечивающей достойный уровень жизни, а также обучение базовым знаниям сотрудников (в том числе повышение их квалификации, переподготовка) в области компьютерной безопасности. Ряд стран, столкнувшись с данной проблемой – нехваткой киберспециалистов, стремится привлекать в сферу кибербезопасности и разведки молодежь, предлагая студентам-выпускникам полугодовую стажировку и финансовую поддержку.

Дания усилила национальную кибербезопасность посредством развития сенсорных сетей и создания ситуационного центра для представления более целостной оперативной картины. С 2020 г. армия США для предотвращения проникновения угроз в армейскую сеть перешла на Windows 12 и обновила текущую версию системы «Статус региональной IT-безопасности».

В Республике Беларусь активно функционируют подразделения по противодействию киберпреступности, входящие в состав криминальной милиции органов внутренних дел. С 2014 г. наблюдается значительный рост киберпреступлений, способы совершения которых весьма разнообразны. Лишь в 2021 г. снизилось их количество по сравнению с 2020 г. (в 2021 г. органами внутренних дел зарегистрировано 16 446 рассматриваемых преступлений, в 2020 г. – 25 561, в 2019 г. – 10 539 таких уголовно наказуемых деяний). В 2021 г. возбуждено около 15 тыс. уголовных дел в сфере высоких технологий, а в 2020 г. – около 24 тыс. уголовных дел данной категории. С каждым годом киберпреступность приобретает более организованный, групповой характер и одновременно характеризуется латентностью. Наблюдается рост хищений с банковских платежных карточек физических лиц.

В условиях пандемии киберпреступники не перестают атаковывать, осуществляя фишинговые рассылки, вынуждая тем самым пользователей сети Интернет открывать зараженные вирусом файлы или ссылки. Это позволяет похитить конфиденциальные данные вплоть до установления контроля над электронным устройством пользователя. Например, Всемирная организация здравоохранения констатировала, что в сети Интернет размещена как достоверная, так и недостоверная информация о пандемии. Хакеры, воспользовавшись такой ситуацией, стали рассылать электронные письма, в которых якобы предлагалась услуга в виде

консультирования медицинскими организациями по вопросам относительно коронавирусной инфекции и средств защиты от нее. Однако это были фишинговые атаки. COVID-19 усложнил ситуацию с обеспечением кибербезопасности, так как большинству населения на планете пришлось во время пандемии перейти на дистанционную работу, используя свои персональные компьютеры дома, забыв о мерах безопасности, которые реализуют работодатели в закрытых корпоративных сетях. Поэтому под угрозой оказываются не только личные данные, но и служебная информация. Чтобы не стать жертвой киберпреступников, необходимо следующее:

обращать внимание на сомнительные электронные письма (грамматические ошибки, неграмотные формулировки), так как большинство рассылок осуществляется из-за границы;

помнить, что часто в фишинговых обращениях подчеркивается срочность действий, необходимость немедленно нажать на ссылку, а также поступающее предложение нереалистично заманчиво.

Так, хакеры группировки Muddy Water попытались взломать компьютеры израильских компаний посредством фишинговой рассылки с использованием зараженных документов в форматах PDF и Excel. Однако своевременно была отражена кибератака и возобновлена работа этих компаний.

В Республике Беларусь в качестве перспективных направлений борьбы с киберпреступностью определены следующие:

подготовлен разработанный совместно МВД Республики Беларусь и Национальным банком Республики Беларусь проект указа Президента Республики Беларусь, в котором прописаны действенные меры по предотвращению кибератак, в частности, в отношении граждан;

в Следственном комитете Республики Беларусь планируется создать спецподразделение по борьбе с киберпреступностью, в компетенцию которого будут входить цифровизация ведомства, расследование преступлений в сфере высоких технологий.

Таким образом, усложнение компьютерных сетей, изощренность действий преступников, распространение коронавирусной инфекции COVID-19 привели к повышенному уровню киберугроз. Мировое сообщество должно быть бдительным и принимать всевозможные меры по недопущению взлома паролей, хищения либо искажения информации, имеющейся в электронных устройствах, вмешательства в работу различных систем посредством сети Интернет, а также совершения иных противоправных действий. Правоохранительные органы постоянно ведут активную работу по выявлению киберпреступников и предотвращению кибератак.