деятельным раскаянием лица, примирением сторон и возмещением причиненного ущерба, что в последующем приводит к росту рецидива преступлений.

Полагается, что ряд проблемных вопросов противодействия цифровой преступности в глобальной компьютерной сети Интернет заключается в следующем: недостаточное поступление в правоохранительные органы количества заявлений потерпевших о совершении рассматриваемого вида преступлений; уровень квалификации сотрудников и финансирование подразделений в сфере борьбы с цифровой преступностью требует определенного повышения; отсутствие на законодательном уровне положений, всесторонне рассматривающих порядок расследования данных преступлений и пр.

Таким образом, сегодня перед государством стоит стратегически важная задача, заключающаяся в разработке эффективных способов противодействия высокотехнологичной преступности в сети Интернет.

Применительно к Республике Беларусь особое внимание целесообразно уделять тщательной предварительной подготовке при проведении осмотра места происшествия, обыска или выемки, использованию специальных технических устройств и программного обеспечения, а также принятию мер по обеспечению сохранности компьютерной информации. Например, проведение такого следственного действия, как прослушивание и запись переговоров (ст. 214 Уголовно-процессуального кодекса Республики Беларусь) по уголовным делам, если имеются достаточные основания полагать, что эти переговоры содержат сведения о преступлении, либо имеющие значение для дела, может способствовать установлению мест нахождения используемой компьютерной техники, иных незаконных предметов, документов (в частности электронных).

Кроме того, весьма важно предусмотреть и специальные меры предупреждения преступлений, совершенных с использованием информационных технологий в сети Интернет. К числу данных мер относятся: повсеместное введение и обеспечение достаточной и обязательной идентификации личности пользователя (включая места общественного пользования интернетом); разработка для каждого пользователя сети Интернет программы предоставления электронного сертификата, в котором будут содержаться все сведения, идентифицирующие личность пользователя; введение процедуры заключения в письменном виде договора с провайдером, способствующее предотвращению регистрации неподписанных электронных ящиков.

Однако противодействовать рассматриваемому роду преступности лишь на национальном уровне малоэффективно, так как принцип территориальности практически неприменим к глобальной компьютерной

сети Интернет. В этой связи одним из важнейших вопросов в сфере противодействия преступлениям, совершаемым с использованием цифровых технологий в сети Интернет, является совершенствование международного взаимодействия в сторону его упрощения, что, в свою очередь, окажет положительное влияние, например, на оперативность исполнения запроса о правовой помощи, а соответственно, и на эффективность противодействия вышеуказанной преступности.

Резюмируя изложенное, очевидно, что противодействие высокотехнологичной преступности в сети Интернет является одним из наиболее злободневных вопросов, стоящих перед современным обществом и государством. Совершенствование порядка расследования, сбора и оценки доказательств, повышение уровня научно-методического обеспечения, а также развитие международного сотрудничества является основой противодействия рассматриваемой преступности.

УДК 343.92

В.В. Лавренов, М.А. Лохницкий

НЕКОТОРЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ ПРИ ПОСТРОЕНИИ ЭФФЕКТИВНОЙ СИСТЕМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ

На нынешнем этапе мирового развития информационная сфера приобретает ключевое значение для современного человека, общества, государства и оказывает всеобъемлющее влияние на происходящие экономические, политические и социальные процессы в странах и регионах.

Наблюдается рост преступности с использованием информационно-коммуникационных технологий. Появился новый вид преступности – киберпреступность. Киберпреступность – это любая преступная деятельность, нацеленная на компьютер, компьютерную сеть или подключенное устройство или использующая ее.

Математическое моделирование является одним из новых направлений в борьбе с преступностью, и за последнее время был предложен ряд моделей, в которых используются различные подходы. Они варьируются от моделей на основе метода когнитивного моделирования до дифференциального моделирования.

При применении метода моделирования выделяют пять этапов:

1) создание репрезентативной среды;

2) тестирование, исследование и оценка;

3) обучение и упражнения;

4) анализ и оценка рисков;

5) изучение роли людей в области кибербезопасности.

Существует тесная связь между этими этапами исследований. Создание репрезентативной среды относится к созданию сетей и подключенных систем. Исследования в области кибербезопасности требуют платформы для тестирования. Для реализации сетевой среды моделирования используются библиотеки и инструменты сетевого моделирования с открытым исходным кодом и коммерческие.

Этап тестирования, исследования и оценки подразумевает, что программные сетевые симуляторы и алгоритмы сетевого трафика могут быть использованы для тестирования конкретных типов кибератак. Это практика запуска симулированных кибератак против программного обеспечения с сетевого трафика, чтобы получить представление обо всех возможных уязвимостях, которыми могут воспользоваться настоящие киберпреступники.

Тестирование на проникновение в киберпространство фокусируется на том, как киберпреступник попытается взломать вашу программную систему, от API-интерфейсов до интерфейсных и внутренних серверов, чтобы выявить слабые места в приложении. Выявление этих слабых мест позволит устранить угрозу безопасности и улучшить программное приложение и сетевую инфраструктуру.

На этапе обучения и упражнения предлагается создание специальных подразделений для проведения тренингов и учений по кибербезопасности. Вопросы необходимости обучения кибербезопасности определены в постановлении Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О Концепции информационной безопасности Республики Беларусь» и в ряде других нормативных правовых актов Республики Беларусь.

Основная цель оценки киберрисков – информировать заинтересованные стороны и поддерживать надлежащие меры реагирования на выявленные риски.

Поэтому на этапе анализа и оценки рисков необходимо определить:

наиболее важные критические объекты информационных технологий;

какая утечка данных окажет серьезное влияние на кибербезопасность (будь то вредоносное программное обеспечение, кибератака или человеческая ошибка);

можно ли выявить все источники угроз;

каков уровень потенциального воздействия каждой выявленной угрозы;

каковы внутренние и внешние уязвимости;

каковы последствия использования этих уязвимостей;

какова вероятность эксплуатации;

какие кибератаки, киберугрозы или инциденты безопасности могут повлиять на способность функционирования системы;

какой уровень риска может быть принят.

Если ответить на эти вопросы, то можно определить, что защищать. Это означает, что могут быть разработаны средства управления ИТ-безопасностью и стратегии защиты данных для устранения рисков.

Заключительный этап – изучение роли людей в области кибербезопасности. Люди – злоумышленники, аналитики по кибербезопасности, системные администраторы и обычные пользователи системы взаимодействуют, формируя киберпространство. Поэтому при изучении кибербезопасности необходимо учитывать каждого из них. Злоумышленниками могут быть дети-скриптеры, хакеры, организованные преступные группы, злоумышленники-инсайдеры, любители или террористы. Их роль в киберпространстве определяется их навыками, знаниями, ресурсами, доступом и мотивами. Технологии улучшили защиту киберсистем; однако защита по-прежнему сильно зависит от того, кто управляет системой, и кто имеет к ней доступ.

Таким образом, на современном этапе развития общества в целом возрастает функция математической науки. Методы математического моделирования в русле этой тенденции должны быть ориентированы на решение многообразных задач киберпреступности и кибербезопасности на ближайшее и отдаленное будущее. Для этого математическая наука должна быть обогащена методологическим арсеналом изучения этих проблем. Анализ применяемых методов математического моделирования позволяет сделать обобщающий вывод о том, что эти методы постоянно обогащаются и развиваются. Применение методов математического моделирования позволит решить прикладную задачу по минимизации рисков от угроз и инцидентов в сфере кибербезопасности.

УДК 004:34 (476)

Д.Н. Лахтиков

КИБЕРПРЕСТУПНОСТЬ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информационная сфера очень сильно эволюционировала, став важной составной частью общества и государства, при этом проблемы криминализации в этой сфере приобрели характер национальных и международных. Преступники используют результаты научного и тех-