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-

нического прогресса в своих целях, что обусловило формирование самостоятельного вида преступлений – киберпреступления.

В настоящее время в белорусском законодательстве в Концепции национальной безопасности Республики Беларусь рост преступности с использованием информационно-коммуникационных технологий определен в качестве внутреннего источника угроз национальной безопасности информационной сфере. При этом в гл. 16 Концепции информационной безопасности Республики Беларусь также подчеркивается, что информационные системы и ресурсы становятся как предметом преступлений, так и средством их совершения. Формируется тотальная зависимость финансового сектора и иных секторов от надежности электронных систем хранения, обработки и обмена данными. В качестве одного из наиболее вероятных источников угроз кибербезопасности рассматривается противоправная деятельность отдельных лиц и преступных групп.

Анализ состояния криминогенной ситуации свидетельствует о том, что по подавляющему большинству преступлений против компьютерной безопасности лица, их совершившие, не установлены. Обусловлено это тем, что преступления данного вида, как правило, носят трансграничный характер и большое количество противоправных деяний совершается с использованием, например, компьютерных систем и интернет-ресурсов, находящихся за пределами страны.

Справедливо отмечает М.А. Простосердов, что в перспективе возможно ожидать дальнейшее нарастание в информационной сфере угроз, как во всем мировом сообществе, так и в отдельном государстве. Недостаточная защищенность информационных ресурсов создает угрозы национальной и международной безопасности в целом, может вести к частичной или полной потере государственного информационного суверенитета. Государство должно быть в состоянии эффективно противостоять им, руководствуясь продуманной комплексной стратегией эффективных скоординированных действий по самым различным направлениям, целенаправленно используя весь имеющийся в его распоряжении арсенал сил и средств, что обусловливает не только определение самих угроз национальной безопасности, но и источников этих угроз.

В свою очередь, киберпреступность в настоящее время является не столько источником угроз информационной безопасности, сколько непосредственно самостоятельной угрозой. Источником угрозы информационной безопасности является фактор или совокупность факторов, способных при определенных условиях привести к возникновению самой угрозы. С одной стороны, преступность как сложное социальное явление детерминируется определенными явлениями, факторами, обстоятельствами, которые, в свою очередь, взаимодействуют друг с другом при активном влиянии самой преступности; с другой – киберпреступления, совершаемые с использованием информационно-коммуникационных технологий, охватывают такие преступления, как, например, преступления против компьютерной безопасности; вымогательство, мошенничество, совершение которых сопряжено с преступлениями против компьютерной безопасности, и др. Подобные преступления характеризуются рядом признаков, среди которых можно выделить следующие: взаимосвязь с другими видами преступности; высокотехнологичный характер (совершение с использованием информационно-коммуникационных технологий, средств компьютерной техники, носителей компьютерной информации, которые выступают орудиями и средствами совершения преступлений); высокая степень латентности, обусловленная различными факторами; трансграничность (позволяет преступнику с территории одного государства совершать преступления в отношении лиц, находящихся в другом государстве); постоянное совершенствование существующих и создание новых информационно-коммуникационных технологий, используемых в качестве орудий и средств совершения преступлений. К таким признакам можно отнести также особые структурные характеристики преступных формирований, дистанционный способ совершения преступлений, связь не только с иными видами преступлений, но и с целым рядом негативных социальных отклонений.

Общественная опасность заключается и в том, что негативные последствия приводят к серьезным финансовым потерям, нарушениям функционирования инфраструктур, реальным жертвам и т. д. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее.

Хотя киберпреступления рассматриваются в качестве новой специфической формы преступлений, они способны причинить вред различным охраняемым уголовным законом общественным отношениям, и это довольно широкая категория, которая охватывает значительный круг разнородных деяний в информационной сфере.

В свою очередь, необходимо отметить, что масштабы киберпреступлений достигли таких размеров, что позволяют называть их на современном этапе самостоятельной угрозой информационной безопасности.

Детерминантами киберпреступлений, как отмечают А.Л. Гогаева, А.С. Лолаева, являются следующие факторы. Возможность извлечения дохода при минимальных затратах и относительно невысоком риске; низкий уровень осведомленности в области информационной безопасности у пользователей систем дистанционного банковского обслуживания и иных средств интернет-платежей; определенная степень ано-

нимности пользователей глобальной компьютерной сети Интернет, существование иных анонимных информационно-телекоммуникационных сетей, таких как сеть Tor и других средств и методов анонимизации пользователей; определенная степень анонимности финансовых операций, проходящих в информационно-телекоммуникационных сетях; наличие программных уязвимостей разного уровня в экономически значимых информационных системах глобальной компьютерной сети Интернет, позволяющих нейтрализовать систему защиты, используя вредоносное программное обеспечение.

Перечисленная совокупность признаков отражает высокую степень общественной опасности данных преступлений и предопределяет потенциальную и реальную возможность нанесения ущерба национальным интересам Республики Беларусь в информационной сфере, т. е. угрозу информационной безопасности.

Таким образом, анализ основных подходов к рассматриваемой проблеме позволяет предложить рассматривать киберпреступность в качестве самостоятельной угрозы информационной безопасности Республики Беларусь. При этом трансформации преступности не только порождают необходимость совершенствования законодательства, но изменения организации и тактики предупреждения, выявления и пресечения киберпреступлений.

УДК 343.2.7

О.О. Лемешевский

О НЕКОТОРЫХ ВОПРОСАХ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СЕТИ ИНТЕРНЕТ

Развитие информационного общества, переход Республики Беларусь к цифровизации, затрагивающей все сферы общественной жизни, неразрывно связанным с усилением значения достоверности информации и культуры общения в сети. В связи с этим появляется большое количество информационных площадок, социальных сетей, форумов, видео- и фотохостингов, обеспечивающих доступ к актуальной информации.

Каждый гражданин Республики Беларусь, в том числе и сотрудники органов внутренних дел, военнослужащие внутренних войск, имеют возможность получать информацию, общаться, обсуждать повестку дня, оставлять комментарии. Следовательно, наличие авторов контента, имеющих умысел доводить недостоверную (часто заранее заготовленную) информацию до своих подписчиков, имеют возможность влиять на эмоциональное состояние людей, их мнение и взгляды на те или иные вопросы.

На данную проблему указал Президент Республики Беларусь Александр Лукашенко 21 сентября 2022 г., принимая с докладом Государственного секретаря Совета Безопасности Республики Беларусь. Он отметил: «Сейчас идет война, прежде всего в сфере информационной безопасности. И здесь подключены должны быть все – от журналиста до Президента. Война войной. Информационная война – это очень опасно в современном мире. Начиная, опять же, от «газеты-районки» и прочей какой-то частной газеты и заканчивая Интернетом. Везде должны активно работать.».

Привлекает внимание в аспекте проблематики нашего исследования положение Концепции национальной безопасности Республики Беларусь, в частности к угрозам национальной безопасности относится «деструктивное информационное воздействие на личность, общество и государственные институты, наносящее ущерб национальным интересам».

Заслуживает внимания в рассматриваемой сфере также Концепция информационной безопасности Республики Беларусь, которая раскрывает такое понятие, как «информационный суверенитет Республики Беларусь».

Информационный суверенитет Республики Беларусь – неотъемлемое и исключительное верховенство права государства самостоятельно определять правила владения, пользования и распоряжения национальными информационными ресурсами, осуществлять независимую внешнюю и внутреннюю государственную информационную политику, формировать национальную информационную инфраструктуру, обеспечивать информационную безопасность.

Основополагающим национальным интересом Республики Беларусь в информационной сфере с точки зрения гуманитарного аспекта является реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации, свободу мнений, убеждений и их свободного выражения, а также права на тайну личной жизни.

В этой связи следует сделать вывод: лица, которые публикуют на информационных порталах недостоверную информацию или оскорбляют граждан в сети (в частности, сотрудников органов внутренних дел и военнослужащих внутренних войск), нарушают информационный суверенитет Республики Беларусь, угрожают национальным интересам и должны понести весомую ответственность согласно законодательству.

Анализ действующего законодательства Республики Беларусь и правоприменительной практики показывает наличие соответствующих