ности таможенных органов и т. д. При этом все информационные системы объединены в единую автоматизированную информационную систему таможенных органов.

Как показывает практика, применение информационных технологий в деятельности таможенных органов позволяет снизить временные затраты на оформление, обеспечить оперативность контроля, тем самым улучшить транзитную привлекательность страны.

Вместе с тем нельзя оставлять без внимания факт, что процесс информатизации таможенной сферы имеет и оборотную сторону – наряду с положительными изменениями возможны и негативные последствия, такие как использование возможностей информационных технологий в противоправных целях. Это ставит вопрос об обеспечении перехода информационной безопасности на новый уровень, тем более, с 1 января 2018 г. вступил в силу новый Таможенный кодекс Евразийского экономического союза (ТмК ЕАЭС), знаменующий собой более высокий этап не только экономической, но и информационной интеграции.

Основными причинами, которые поднимают актуальность вопросов обеспечения информационной безопасности на единой таможенной территории Евразийского экономического союза (ЕАЭС), являются:

объединение в единое информационное пространство деятельности таможенных органов государств – членов ЕАЭС, включая сопряжение их информационных систем;

динамичное развитие информационных технологий в таможенном деле, которые требуют новых адаптированных к ним подходов по обеспечению безопасности информации;

закрытость технологий и средств защиты конфиденциальной информации таможенных органов, в том числе национальной государственной тайны.

Анализ существующих подходов государств – членов ЕАЭС в решении задач по обеспечению безопасности информации показал, что они имеют в целом одни и те же взгляды на эту сферу деятельности. Так, в ТмК ЕАЭС содержится ряд норм, в которых отражены положения по регулированию деятельности таможенных органов в сфере обеспечения безопасности информации, в частности этим вопросам посвящены гл. 48 и 49.

Следует отметить, что ТмК ЕАЭС в вопросах обеспечения информационной безопасности сохранил те же подходы, которые в свое время были закреплены в действующем Таможенном кодексе Таможенного союза. Это касается, прежде всего, основополагающих положений обеспечения таможенными органами информационной безопасности:

целевое назначение получаемой таможенными органами информации (любая информация, полученная таможенными органами, используется таможенными органами исключительно для выполнения возложенных на них задач и функций);

запрет на разглашение, использование в личных целях либо передачу иным лицам получаемой таможенными органами информации;

законодательно закрепленный порядок обмена информацией между таможенными органами.

Однако надо иметь в виду, что при реализации указанных положений необходимо решить ряд вопросов, среди которых можно выделить такие, как:

1) соблюдение конституционных прав и свобод граждан в области получения и использования таможенной информации;

2) информационное обеспечение деятельности ЕАЭС, связанное с доведением до населения государств – членов ЕАЭС и международной общественности достоверной информации о его деятельности, его официальной позиции по значимым вопросам в таможенной сфере, с возможностью доступа граждан к его открытым информационным ресурсам;

3) применение и развитие современных информационных технологий собственного производства;

4) защита информационных ресурсов и информационно-телекоммуникационных технологий от угроз в сфере информационной безопасности.

Это, в свою очередь, подразумевает дальнейшее совершенствование и проведения единой политики в области обеспечения безопасности таможенных органов в условиях ЕАЭС, разработки практических мер по воплощению политики безопасности информации и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации.

УДК 004.315.5

С.Н. Касанин

НАУЧНО-МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ В ОБЛАСТИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

В Указе Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь» выделены концептуальные источники угроз национальной безопасности в информационной сфере, на решение которых и направлены наши усилия.

В Указе Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации» четко определено, в каких целях организуются и проводятся научно-исследовательские и опытно-конструкторские работы в сфере технической и криптографической защиты информации.

Приказом Государственного комитета по науке и технологиям Республики Беларусь от 30 мая 2016 г. № 93 утверждена государственная научно-техническая программа «Развитие методов и средств системы комплексной защиты информации и специальных технических средств», 2016–2020 годы.

Эти документы в области технической защиты информации гармонично дополняют и другие соответствующие нормативные правовые акты.

Анализ состояния дел в сфере технической защиты информации показывает:

1. Сложились вполне сформировавшаяся концепция и структура, основу которой составляют:

актуальная и проработанная законодательная база, где достаточно четко очерчена система взглядов на эту сферу деятельности;

весьма развитый арсенал технических средств защиты информации, производимых на промышленной основе;

большое число фирм, специализирующихся на решении вопросов технической защиты информации;

наличие значительного практического опыта и др.

2. Эффективность и соразмерность мер, предпринимаемых в Республике Беларусь, позволяет обеспечить защиту информации от утечек по техническим каналам в соответствии с требованиями действующих нормативно-методических документов и технических нормативных правовых актов.

Несмотря на все предпринятые в законодательстве меры, тем не менее, злоумышленные действия с информацией не только не уменьшаются, но и имеют достаточно устойчивую тенденцию к росту.

Исследования в данной области свидетельствуют, что для борьбы с этой тенденцией нельзя ограничиваться отдельными и разовыми мероприятиями. Необходим системный подход, немаловажное и первостепенное значение в котором отводится непрерывному развитию и совершенствованию научно-методологических аспектов в области технической защиты информации.

Во-первых, необходима проработка и конкретизация приоритетных научных исследований в области технической защиты информации.

Анализ структуры ведущих разведок мира позволяет сделать вывод о том, что подразделения, занимающиеся добыванием информации по

техническим каналам, а также вопросами преодоления программных и аппаратных средств защиты в сфере информационных технологий, играют более важную роль, чем подразделения традиционной разведки.

Научные исследования в данной области не должны стоять на месте, требуется четкое взаимодействие и участие в этом процессе: государственных и коммерческих организаций, специальных служб, которые способны предоставить информацию специалистам данного направления.

Необходимо адекватное выявление моделей угроз информационной безопасности. Требуется дальнейшая проработка вопросов количественной оценки рисков и преимуществ, основанной на рациональных математических моделях.

Исследования и результаты работ по этому направлению зачастую являются коммерческой тайной. Однако доступные исследования, как, впрочем, и сам факт защиты информации о методиках оценки информационной безопасности, указывают на актуальность исследований в данной области.

Приоритетными научными исследованиями в области технической защиты информации, на наш взгляд, должны стать следующие направления:

1. Исследование места и роли проблем технической защиты информации в становлении современного информационного общества.

2. Разработка и научное обоснование системы мониторинга состояния технической защиты информации.

3. Совершенствование нормативно-методической базы проведения экспертизы и контроля качества защиты информации.

4. Проблемы формирования международной системы в области технической защиты информации.

5. Исследования, направленные на создание комплекса отечественных инструментальных средств проектирования средств технической защиты информации.

6. Разработка и совершенствование моделей угроз безопасности, систем и способов их реализации, определение критериев уязвимости и устойчивости систем к деструктивным воздействиям, разработка методов и средств мониторинга для выявления фактов применения несанкционированных информационных воздействий, разработка методологии и методического аппарата оценки ущерба от воздействия угроз информационной безопасности.

7. Анализ возможности использования достижений физики и техники для получения доступа к информации, обрабатываемой на современных технических средствах, в том числе исследование физических основ утечки информации от технических средств по побочным каналам, разработка проблем аналитической обработки побочных сигналов.

8. Исследование алгоритмических и технологических особенностей новейших зарубежных и отечественных технических средств обработки информации.

9. Разработка методологии оценивания защищенности, комплексных методов и средств защиты технических средств обработки информации от физико-технических методов несанкционированного доступа, совершенствование соответствующей нормативной базы.

10. Сравнительный анализ тенденций развития физико-технических проблем защиты информации в стране и за рубежом.

11. Разработка и научное обоснование моделей угроз и стратегий защиты объектов от технических разведок.

12. Разработка методов и средств противодействия техническим разведкам с учетом эффективности функционирования.

13. Разработка методов и средств контроля состояния и достаточности принимаемых мер по противодействию техническим разведкам на объектах защиты.

Во-вторых, значимой для развития исследований в области технической защиты информации остается проблема хронического недофинансирования.

С целью минимизации пробелов в данном направлении, целесообразно разработать меры по стимулированию:

публикационной и патентной активности исследователей;

привлечения молодежи в исследовательскую деятельность;

привлечения бизнес-организациями молодых ученых к выполнению научных исследований в области информационной безопасности.

Одним из ключевых условий научного и технологического развития в области технической защиты информации должно стать участие крупных компаний. Поддержка научной деятельности – важнейший фактор сохранения коммерческой тайны и удержания сферы влияния на отечественном и мировом рынках. Кроме того, обеспечивается устойчивое финансирование научных организаций, которое позволяет формировать новые знания.

В-третьих, необходимо совершенствование кадровой политики в сфере технической защиты информации.

Существенное противодействие росту компьютерных преступлений может оказать грамотная политика в подборе и подготовке национальных кадров в сфере информационной безопасности.

Проведенные социологические исследования студентов и специалистов, работающих в области защиты информации, позволяют сделать следующие выводы:

1. Дерзость совершения компьютерных правонарушений у молодежи вызывает восхищение, желание самоутвердиться, показать себя с

лучшей стороны и привлечь к себе внимание. Среди других факторов, определяющих желание осуществлять компьютерные правонарушения, можно выделить желание заработать.

2. Многие абитуриенты, поступая на специальности, связанные с защитой информации, преследуют корыстную цель – научиться методам совершения компьютерных преступлений.

3. Подавляющее большинство студентов, обучающихся на специальностях, связанных с вычислительной техникой, очень слабо знают нормативные правовые документы по защите информации.

Анализ информации позволил выявить ряд условий, реализация которых даст возможность обеспечить качественную подготовку специалистов в области технической защиты информации.

Для выработки рекомендаций по совершенствованию подготовки специалистов в области технической защиты информации необходимо выделить три направления: учебно-воспитательное, учебно-методическое, организационно-административное.

Немаловажной задачей становится повышение квалификации специалистов в области защиты информации.

Приоритетным направлением должна быть подготовка кадров высшей научной квалификации, которые проводили бы исследования в области технической защиты информации.

УДК 343.985

А.А. Ковальчук

КЛАССИФИКАЦИЯ ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНОЙ ТЕХНИКИ

В настоящее время жизнь людей буквально невообразима без привычных программно-технических средств, например компьютеров, которые позволяют автоматизировать сложнейшие процессы и существенно расширить человеческие возможности. Однако далеко не всегда достижения науки и техники используются во благо. Нередко отдельные представители общества, руководствуясь корыстными и иными деструктивными мотивами, совершают различного рода противоправные деяния.

На современном этапе широкое распространение получили хищения, совершаемые с использованием компьютерной техники. Впервые подобные преступления были выявлены на территории Республики Беларусь на рубеже прошлого и нынешнего веков и основывались на незаконном использовании банковских платежных карточек (БПК). В дальнейшем с развитием информационных технологий происходил процесс эволюции способов совершения хищений.