Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

НАУЧНО-МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ В ОБЛАСТИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

А.Н. ГОРБАЧ, С.Н. КАСАНИН

Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации»

В Указе Президента Республики Беларусь от 09.11.2010 № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь» выделены концептуальные источники угроз национальной безопасности в информационной сфере на решение которых и направлены наши усилия:

Внутренние источники угроз национальной безопасности:

распространение недостоверной или умышленно искаженной информации, способной причинить ущерб национальным интересам Республики Беларусь;

зависимость Республики Беларусь от импорта информационных технологий, средств информатизации и защиты информации, неконтролируемое их использование в системах, отказ или разрушение которых может причинить ущерб национальной безопасности;

несоответствие качества национального контента мировому уровню;

недостаточное развитие государственной системы регулирования процесса внедрения и использования информационных технологий;

рост преступности с использованием информационно-коммуникационных технологий;

недостаточная эффективность информационного обеспечения государственной политики;

несовершенство системы обеспечения безопасности критически важных объектов информатизации.

Внешние источники угроз национальной безопасности в научно-технологической сфере:

ограничение доступа белорусских исследователей и субъектов хозяйствования к новейшим технологиям, результатам исследований и разработок мирового уровня;

целенаправленная политика иностранных государств и компаний, стимулирующая эмиграцию высококвалифицированных ученых и специалистов из Республики Беларусь.

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:

изучения и анализа современных тенденций развития методов и средств технической и криптографической защиты информации;

создания нормативной правовой базы в сфере технической и криптографической защиты информации;

оценки вероятных и актуальных видов угроз защищаемой информации, а также определения оптимальных способов противодействия угрозам защищаемой информации;

обоснования необходимой степени защищенности объектов, на которых осуществляется техническая и криптографическая защита информации;

разработки предложений по формированию единой политики по технической и криптографической защите информации;

создания перспективных отечественных методов и средств защиты информации;

научно-методического обеспечения подтверждения соответствия средств защиты информации требованиям технических нормативных правовых актов.

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 (ГНТП «Защита информации – 3»), на 2016 – 2020 годы.

Основные цели ГНТП «Защита информации:

совершенствование нормативно-методической базы в области ЗИ;

разработка и совершенствование высокопроизводительных средств защиты информации, средств оценки степени защищенности информационных систем, специальных технических средств;

создание научно-технических условий для эффективного обеспечения безопасности информации на критически важных объектах информатизации и повышения степени защищенности объектов информатизации, систем связи и передачи данных;

обеспечение импортозамещение средств защиты информации и специальных технических средств.

Эти документы в области технической защиты информации гармонично дополняют и другие соответствующие НПА.

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 очерченная 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 другое.

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

Не смотря на все предпринятые в законодательстве меры, тем не менее, злоумышленные действия над 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. Это непрерывный процесс, немаловажное и первостепенное значение в котором отводится развитию и совершенствованию научно-методологических аспектов в области технической защиты информации.

Первое: Необходима проработка и конкретизация приоритетных научные исследования 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 наиболее важную роль, чем подразделения традиционной разведки.

Более того, многие ведущие страны мира выделяют такие подразделения в самостоятельные службы (АНБ США, ЦПС Великобритании и т.п.), бюджет которых ино-

гда значительно превосходит бюджет подразделений традиционной разведки, понятно, что ни одна спецслужба не станет сворачивать свои программы в данной области.

Таким образом, в XXI веке техническая разведка не только не потеряет своей значимости, но и поднимется на качественно иную ступень развития по созданию:

сверхминиатюрных технических устройств, предназначенных для скрытого проникновения на нужной разведке объекты и получения информации;

систем искусственного интеллекта, которые смогли бы в автоматическом режиме вести смысловой анализ информации, выявляя в ней скрытый смысл, и другие работы в области высоких технологий.

Вот почему роль средств и методов технической защиты информации будет все больше и больше усиливаться.

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 представить информацию специалистам данного направления.

Необходимы адекватные модели выявления угроз информационной безопасности. Требуется дальнейшая проработка вопросов количественной оценки рисков и преимуществ, основанная 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 их функционирования.

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

Второе: Значимой для развития исследований в области технической защиты информации остается проблема хронического недофинансирования.

Фактор недофинансирование влияет на формирование неблагоприятной исследовательской среды, снижение производительности труда исследователей и как итог уход из данной сферы деятельности.

Накопленные за прошедший период проблемы обусловили невысокий уровень производительности труда исследователя в научных организациях. Прежде всего, на производительность труда исследователей оказывает влияние наличие устаревшего оборудования и технологий; наличие большого количества бюрократических барьеров; недостаточная мотивация исследователей и отсутствие конкурентоспособных государственных программ.

С целью минимизация пробелов данном направлении, целесообразно:

1. Разработать рекомендации для научных и образовательных организаций по реализации комплекса мер стимулирования публикационной и патентной активности исследователей.

2. Разработать государственные меры стимулирования процессов привлечения молодежи в исследовательскую деятельность.

В том числе меры стимулирования должны включать: систему грантов для молодых ученых, участвующих в исследовательских проектах научных организаций; создание «временных» ставок для аспирантов в научных организациях; формирование исследовательской аспирантуры для предоставления более широких возможностей при выборе аспирантом своей карьерной траектории; развитие системы обеспечения молодых учёных жильём; стимулирование деятельности академических и вузовских учёных в сфере популяризации науки и распространения научных знаний в молодёжной среде; повышение престижа профессии ученого через продвижение науки и научного знания в СМИ; нематериального мотивирования молодых ученых.

3. Разработать государственные меры стимулирования бизнес-организаций по привлечению молодых ученых к выполнению научных исследований в области информационной безопасности.

Немаловажное значение имеет то, что в заказе на результаты научных исследований в области ТЗИ необходимо активней привлекать бизнес.

Одним из Ключевых элементов научного и технологического развития в области технической защиты информации должны является крупные компании.

Поддержка научной деятельности для них важнейший фактор в области сохранения коммерческой тайны и удержания сферы влияния на отечественном и мировом рынке. При этом обеспечивается устойчивое финансирование научных организаций, которое позволит формировать новые знания.

Третье: Совершенствование кадровой политики в сфере ТЗИ.

Существенное противодействие росту преступлений в сфере информационных технологий может оказать грамотная политика подбора и подготовки 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. Часто хакеры совершают взломы сети, чтобы произвести впечатление на окружающих. 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 нормативно-правовые документы по защите информации, в частности, они практически не знают, какую ответственность несет злоумышленник за совершение компьютерных преступлений.

Анализ информации, позволил выявить ряд условий, реализация которых позволит 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.

1. Учебно-воспитательное направление совершенствования процесса подготовки специалистов в технические защиты информации.

Одним из важных факторов повышения качества подготовки специалистов в области технической защиты информации должны быть меры по ужесточению режима отбора для обучения.

Можно предложить следующие пути развития технологии профотбора:

1) создание эталонных моделей студента и специалистов в многомерном пространстве профессионально важных качеств;

2) отражение в содержании профессионально важных качеств познавательных способностей личности, адаптационных возможностей в профессиональной направленности кандидата;

3) разработка алгоритма оценки близости реальных и эталонных образцов кандидата с расчетом, как обобщенного интегрального показателя, так и уровней развития составляющих каждого показателя.

3.2. Учебно-методическое направление совершенствования процесса подготовки специалистов в области технические защиты информации

Обеспечение тесной связи учебного процесса с научными исследованиями в области информационной безопасности.

Для отражения современных достижений в области технической защиты информации необходимо регулярно пересматривать содержание специальных учебных дисциплин.

3.3. Организационно-административное направление совершенствования процесса подготовки специалистов в области технические защиты информации.

Один из путей – жесточайший контроль качества обучения (уровня подготовки), сертификация руководящего и преподавательского состава учебного заведения.

Немаловажной задачей является Повышение квалификации специалистов в области защиты информации

В настоящее время одной из проблем повышения квалификации является низкий уровень профессиональной подготовки руководящих работников структурных подразделений. Встречаются случаи, когда подразделениями повышения квалификации руководит человек не имеющего не только подготовки в области информационной безопасности, но и вообще компьютерного образования, к тому же и нет опыта преподавательской работы.

Одним из путей совершенствования процесса повышения квалификации – проведение аттестации лиц, занимающихся подготовкой (переподготовкой) кадров. Они должны иметь обязательную специализированную подготовку и иметь опыт преподавательской работы.

Штатные преподаватели системы переподготовки кадров и повышения квалификации в полной мере не могут дать навыков и опыта в силу тех же причин, что и преподаватели базового образования.

Приоритетное направление – подготовка кадров высшей научной квалификации, которые бы проводили исследования в области технической защиты информации.

ЕДИНСТВО НАУЧНОГО ЗНАНИЯ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

В.К. ЖЕЛЕЗНЯК, Д.С. РЯБЕНКО

Полоцкий государственный университет

«Всякое исследование основано на научной интуиции, экспериментальном искусстве, верном ощущении возможности техники и, что весьма важно, – на хорошем знании теории; только при овладении внутренними взаимосвязями явлений представляется возможным обозреть всю совокупность различных проблем и найти путь решения той или иной возникшей проблемы».

Е. Скучик [1]

Решение комплексной защиты информации является приоритетной научной и практической задачей. Теоретические и экспериментальные исследования основаны на логических методах моделирования (математического и физического), абстрагирования и обобщения. Научные знания устанавливают определенность научных результатов в оценке защищенности объектов информатизации, информационных автоматизированных систем, входящих в объект информатизации, проверенных при экспериментальных исследованиях на практике. Высокоточные малоинерционные автоматизированные системы измерения, методы обработки и анализа семантической информации (речевая, видео, передача данных) с высокой степенью определенности, воспроизводимости, обоснованности при влияющих факторах среды распространения, маскирующими сигналами, целостным и системным представлением является айсбергом поучения новых знаний, характеризующиеся истинностью и полезностью.

Методология познания определяется формированием основанных на опыте и интуиции абстрактных представлений, проверяемых практикой. Основным является выделение наиболее существенных свойств и признаков явления или объекта, выделение новых наиболее существенных для теоретического и экспериментального исследования формированием модели. Практическая полезность выводов формирует критерий адекватности цели исследований.