ИНФОРМАТИКА

2004 октябрь-декабрь №4

УДК 681.3.004.056.53

В.В. Анищенко, В.К. Фисенко

ОТ КОНЦЕПЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДО БЕЗОПАСНОСТИ СУПЕРКОМПЬЮТЕРНЫХ СИСТЕМ

Приводится анализ этапов становления и развития исследований в области информационной безопасности, проводимых в ОИПИ НАН Беларуси, показаны полученные на этих этапах результаты.

Введение

В условиях формирования современного информационного общества большое значение приобретает проблема информационной безопасности. Она возникает на разных уровнях (обеспечение информационной безопасности государства, организации или частного лица) и определяет сегодня одно из основных направлений развития информационных технологий (ИТ). Указанная мировая тенденция в полной мере характерна и для Беларуси. Это подтверждает тот факт, что начиная с 1995 г. в Беларуси планомерно ведутся работы в области информационной безопасности как в рамках пятилетних государственных научно-технических программ (шифр «Защита информации»), так и в рамках других программ, например «СКИФ», «Космос» и др. В 2002 г. Совет Министров Республики Беларусь утвердил Государственную программу «Электронная Беларусь», которая в качестве одного из приоритетных направлений развития информатизации включает создание новых средств защиты информации, направленных на совершенствование системы информационной безопасности страны.

В лаборатории проблем защиты информации ОИПИ НАН Беларуси исследования в области информационной безопасности ведутся с 1993 г. по настоящее время. Этот период можно разбить на четыре этапа:

- формирование системы взглядов на решение проблемы информационной безопасности;
- комплексное решение проблемы информационной безопасности;
- создание нормативно-методической базы обеспечения информационной безопасности;
- аттестация объектов информатизации и сертификационные испытания продуктов и систем информационных технологий.

Кратко рассмотрим каждый из этих этапов.

1. Формирование системы взглядов на решение проблемы информационной безопасности

Проблема защиты информации возникла в конце 1950-х гг., когда появились системы электронной обработки данных. Следует отметить, что до 90-х гг. прошлого столетия работы в области защиты информации были под строгим государственным контролем и достижения науки в этой области были доступны узкому кругу ученых. Для специалистов ИТК АН Беларуси (ныне ОИПИ) первыми доступными работами в рассматриваемой области были специальные выпуски журнала «Зарубежная радиоэлектроника», затем стали частично доступны Оранжевая книга, Красная книга, Европейские критерии, Канадские критерии, Федеральные критерии и, наконец, Международный стандарт оценки безопасности информационных технологий [1]. Решением Государственного центра безопасности информации институт был определен головной организацией по разработке Концепции создания Государственной системы защиты информации. Кроме того, лаборатория проблем защиты информации принимала участие в разработке Концепции национальной безопасности Республики Беларусь (раздел «Информационная безопасность»), Концепции информационной безопасности Беларуси, Концепции информационной безопасности СНГ. Вопросы и предложения, связанные с разработкой концепций, докладывались на конференциях и публиковались в различных изданиях [2–4]. Самым сложным в работе

над концепциями был вопрос раскрытия сути проблемы. Известно, что проблема возникает в том случае, если существуют противоречия между людьми, государствами, процессами и т. д. Учитывая эти противоречия, проблема защиты информации получила следующую трактовку: широкое распространение и повсеместное применение вычислительной техники значительно способствовали экономическому и научному прогрессу человечества, а с другой стороны, повысили уязвимость обрабатываемой информации, которая проявилась в подверженности физическому уничтожению или искажению, возможности несанкционированной (случайной или злоумышленной) модификации, а также опасности несанкционированного (случайного или злоумышленного) получения ее лицами, для которых она не предназначалась.

Коротко эта проблема формулируется как обеспечение целостности, доступности и конфиденциальности активов информационной системы, или защита от несанкционированного доступа (НСД).

В процессе разработки концепции выявилась еще одна проблема защиты информации. Бурное развитие информатики способствовало также ускоренному развитию технических устройств и систем разведки. Довольно часто, и это подтверждается многочисленными фактами, выгоднее потратить определенную сумму на добывание уже существующей технологии, чем в несколько раз больше денежных и материальных средств на создание собственной. А в политике и в военном деле выигрыш иногда оказывается просто бесценным. Рассмотрим эту проблему подробнее.

Работа вычислительной техники сопровождается электромагнитными излучениями и наводками на соединительные провода, цепи питания, телефонные линии и т. д. Электромагнитные излучения могут быть приняты средствами разведки и затем декодированы. Наводки электромагнитных излучений могут быть приняты и декодированы путем подключения к линиям связи, проводам заземления и т. д. Так появилась проблема противодействия иностранным техническим разведкам. Этот термин по мере снятия «железного занавеса» исчезает из употребления, однако проблема защиты остается и называется защитой информации от утечки по техническим каналам.

Выявлено также противоречие между пространственным расширением информационных систем, в том числе созданием глобальных сетей, возможностями информационного обмена между разнесенными на большие расстояния государствами и наличием уязвимостей информационных систем, которое позволяет нарушителю ввести в программное обеспечение несколько десятков строк программ-вирусов, чтобы глобальная система стала неуправляемой. Так появилось третье направление решения проблемы информационной безопасности – защита информации и ресурсов от программ-вирусов.

Для решения указанных проблем правительством Республики Беларусь была создана Государственная система защиты информации (ГСЗИ), которая действует по настоящее время. План мероприятий по реализации Концепции создания ГСЗИ содержал задачу разработки Государственной научно-технической программы. В разработке и реализации первой программы институт принял активное участие в качестве головной организации.

После разработки Концепции создания ГСЗИ и других концепций возникла необходимость в создании Концепции информационной безопасности для Национального банка Республики Беларусь. С этой работой специалисты института успешно справились. Результаты разработок неоднократно публиковались и докладывались на конференциях и семинарах [5–8]. Так завершился первый и начался второй этап решения проблемы информационной безопасности.

2. Комплексное решение проблемы информационной безопасности

Второй этап совпадает по времени с выполнением первой Государственной научно-технической программы «Развитие методов и средств комплексной защиты информации» (шифр «Защита информации») и выходом в свет первой версии Критериев оценки безопасности информационных технологий. По программе «Защита информации» институт выполнял следующие задания:

- разработка научно-методологических основ комплексной защиты информации;
- создание межсетевого экрана для безопасного подключения ЛВС к открытым вычислительным сетям (ОКР «Экран-1»);

- создание системы контроля и обнаружения удаленных сетевых атак (ОКР «Мониторинг»);

- разработка аппаратно-программного комплекса средств защиты информации от НСД с применением средств криптографии (ОКР «Доступ»);

- разработка комплекса моделей синтеза и анализа требований безопасности информационных технологий (НИР «Модель»).

На основе полученного опыта впоследствии были осуществлены:

- обоснование требований безопасности к картографическому центру Минобороны Республики Беларусь;

- обоснование требований безопасности к суперкомпьютерному центру кластерного уровня и разработка Положения по обеспечению безопасности информации, обрабатываемой в суперкомпьютерном центре коллективного пользования.

Задачи первого направления решались в НИР «Поиск», а также в рамках фундаментальных исследований в области обнаружения аномальной активности в отношении информационной безопасности.

При исследовании научно-методических основ защиты информации было показано, что обеспечение информационной безопасности не может быть просто сведено к совокупности даже очень эффективных, но не связанных между собой средств и систем защиты информации. Ранее используемый принцип «против конкретной угрозы – конкретное средство защиты» не только не гарантирует защиту системы в целом, но может характеризоваться избыточностью средств защиты, а значит ее высокой ценой, которая, возможно, превысит стоимость защищаемых активов. Были сформулированы два фундаментальных принципа обеспечения информационной безопасности:

- интегрированности, в соответствии с которым информационная безопасность обеспечивается сплошной комплексной структурой, объединяющей построенные на базе информационных технологий средства контроля, передачи и обработки информации, управления механизмами защиты информации и окружающей среды, а также набор гармонизированных законодательных и нормативных актов и организационных мероприятий, определяющих действия персонала информационных систем и службы безопасности;

- комплексности, в соответствии с которым информационная безопасность обеспечивается только при комплексном учете всей совокупности неблагоприятных факторов, угроз активам, возможных каналов утечки и компрометации информации, перспективных средств и методов защиты информации и окружающей среды.

В соответствии с указанными принципами в 1996–1998 гг. был переработан ряд документов бывшего СССР и разработаны вновь основополагающие (на тот период) документы в области безопасности информационных технологий (всего 36 документов), в частности документы, содержащие нормы эффективности защиты; категории объектов информатизации; профили защиты для объектов, обрабатывающих информацию различного уровня секретности; описание системы поддержки принятия решений по формированию профилей защиты и заданий по безопасности и др.

Необходимо отметить, что по методологическому направлению впервые в Беларуси была издана книга «Компьютерная преступность и информационная безопасность» [3], в которой автором раздела «Методологические основы оценки безопасности информационных технологий» является руководитель лаборатории проблем защиты информации В.В. Анищенко. В лаборатории был разработан комплекс моделей количественной оценки безопасности продуктов и систем информационных технологий [9, 10]. В основе комплекса лежит метод оценки эффективности защиты информации, признанный в институте лучшим научным результатом 2000 г. в области фундаментальных исследований.

Наиболее существенные результаты исследований лаборатории были достигнуты по следующим направлениям:

- общие вопросы информационной безопасности [11–13];

- сертификация продуктов и систем информационных технологий [14, 15];

- аттестация объектов информатизации по требованиям информационной безопасности [16, 17];

- обнаружение атак на информационные системы [18–21];

- стандартизации объектов информационной безопасности [22, 23];
- обоснование требований безопасности [24–26].

ОКР «Экран-1», выполненная специалистами лаборатории, была посвящена разработке структуры, алгоритмов и базовых программных средств межсетевого экрана канального, сетевого и транспортного уровней для обеспечения информационной безопасности локальных вычислительных сетей при их взаимодействии с глобальными вычислительными сетями. Ядром межсетевого экрана (МЭ) является экранирующая подсистема (ЭП), реализованная на платформах Windows NT и Linux. ЭП включает API и фильтр пакетов TCI/IP. API – это перечень соглашений по параметрам и алгоритму взаимодействия между сервером доступа к ЭП и фильтром пакетов TCI/IP. API является платформонезависимым, т. е. его спецификации для ОС Windows NT и Linux одинаковые. Фильтр пакетов TCI/IP загружает параметры фильтрации, обрабатывает пакеты TCI/IP, уведомляет об атаке и изменении своего состояния и включает фильтр уровня ядра, уровня приложений и динамические базы реализации правил фильтрации и политики безопасности. Фильтр уровня ядра логически располагается между драйверами сетевых карт и драйвером сетевого протокола TCI/IP. Он перехватывает все кадры Ethernet, осуществляет их фильтрацию и передает на обработку фильтру уровня приложений. Сервер доступа к ЭП работает на платформе Windows NT. На нижнем уровне он взаимодействует с фильтром пакетов TCI/IP. Взаимодействие с фильтром пакетов на платформе ОС Linux осуществляется через API по протоколам TCI/IP. Административная (управляющая) система представлена совокупностью подсистем администрирования, аудита, генерации отчетов и уведомления о нарушении информационной безопасности. Ее взаимодействие с ЭП осуществляется по схеме клиент–сервер с использованием программной системы Connection Manager 2.0 для обеспечения безопасного доступа администратора МЭ к ЭП. Результаты работы опубликованы в [27–29].

ОКР «Мониторинг» посвящена созданию опытных образцов программных комплексов мониторинга и управления безопасностью локальных вычислительных систем при их взаимодействии со службами сети Интернет. Пакет программных средств обеспечивает перехват TCP/IP пакетов, проходящих в локальной сети, запись, фильтрацию и анализ перехваченных пакетов, проверку корректности перехваченных данных, анализ трафика локальной сети на предмет обнаружения атак на сетевые службы, анализ доступа к недекларируемым типам сервисов, проверку нарушения структуры пакетов, анализ подмены сетевых реквизитов, формирование статистической информации и протокола работы, интерактивное управление сетевыми устройствами. Данный комплекс может функционировать как на защищаемом объекте (сервере, ПЭВМ), так и на удаленном рабочем месте администратора безопасности информационной системы. В перечень обнаруживаемых атак входили все известные на тот момент виды явного и скрытого сканирования портов, атаки на отказ в обслуживании (DOS-атаки), ICMP-smurf-атаки, PING-flood-атаки. Принцип работы подсистемы обнаружения атак состоит в «прослушивании» сетевого трафика, селективном кэшировании передаваемой информации и дальнейшем эвристическом анализе кэша относительно статуса события. На административную консоль могут выдаваться как сообщения о всех сетевых событиях, так и сообщения о совершаемых атаках в зависимости от выбранной конфигурации. Данная система была введена в эксплуатацию в ряде государственных организаций, результаты опубликованы в работах [30, 31].

Аппаратно-программный комплекс средств защиты информации (АПКСЗИ) от НСД разработан в рамках ОКР «Доступ». В зависимости от требований пользователя АПКСЗИ выполняет следующие функции: защиту от НСД с блокировкой ПЭВМ в случае отсутствия или несоответствия карты-ключа пользователя; управление ресурсами ПЭВМ; определение целостности служебной информации и информации пользователей; шифрование информации логических дисков; шифрование служебной информации; хранение служебных ключей и ключей пользователей; организацию фискальных операций; сбор, накопление, просмотр и архивирование журнала регистрации событий. АПКСЗИ состоит из аппаратного модуля и программного комплекса. Аппаратный модуль содержит микропроцессор, обеспечивающий логику работы; энергонезависимую память для хранения таблиц описания пользователей и другой служебной информации; узел взаимодействия с картой-ключом; узел стыка с шиной ПЭВМ и оперативным запоминающим устройством, выполняющих функции буфера обмена, а также аппаратный датчик

случайных чисел. Программный комплекс состоит из следующих блоков: ядра управляющей программы микроконтроллера; программ микроконтроллера, хранимых во флэш-памяти; драйверов, программ тестирования и диагностики; программ инсталляции и переопределения конфигурации; программ защиты от трассировки и дизассемблирования. Отдельные результаты ОКР «Доступ» опубликованы в [32, 33].

В ходе выполнения НИР «Модель» [34–38] разработаны:

- автоматизированная система синтеза, анализа требований и управления информационной безопасностью продуктов и систем информационных технологий;
- комплекс моделей интеллектуализированной системы поддержки принятия решений при анализе выполнения требований безопасности и прогноза ущерба от реализации угроз безопасности;
- комплекс моделей количественной оценки безопасности продуктов и систем информационных технологий.

Полученные на втором этапе результаты показали, что специалисты в области информационной безопасности института способны решать довольно сложные научные и практические задачи, однако при этом был выявлен также ряд концептуальных недоработок в подходах к решению подобных задач. Во-первых, комплексный подход к решению проблемы, обоснованный в рамках НИР «Поиск», и разработанные в НИР нормативно-методические документы не нашли своего практического применения в рамках выполненных других работ. Разработанные программные средства лишь «закрывали» определенные бреши безопасности информационных систем, не решая проблему в целом. Поэтому только некоторые результаты нашли практическое применение, и не из-за их оригинальности или эффективности, а лишь потому, что других средств защиты в Беларуси в то время еще не было. Во-вторых, было допущено ошибочное представление о порядке реализации результатов НИР и ОКР. В СССР после завершения НИР или ОКР существовал этап реализации и внедрения результатов. Данный этап был плановым и финансируемым. В ГНТП «Защита информации» такие этапы не предусмотрены, из-за чего большинство результатов, особенно в части нормативно-методических документов, не были реализованы. В Беларуси к этому времени уже функционировала ГСЗИ, однако основной ее орган – Государственный центр безопасности информации – не был наделен правами введения в действие хотя бы методических документов. В настоящее время лишь Государственный стандарт Республики Беларусь наделен правами ввода в действие нормативно-методических документов в качестве предстандартов и стандартов. Так как стандарты определяют как технические, так и методические направления совершенствования информационной безопасности, то институт в 2001 г. основные усилия направил на создание стандартов в области информационной безопасности. К этому времени был сделан перевод с английского на русский язык ряда международных документов, которые, как показала практика, могут служить хорошей базой для создания национальных стандартов. Наступил третий этап решения проблемы информационной безопасности.

3. Создание нормативно-методической базы обеспечения информационной безопасности

Созданию нормативно-методической базы были посвящены НИР «Разработать научно-методические основы сертификации и аттестации продуктов и систем информационных технологий по требованиям информационной безопасности» (шифр «Сертификат») и «Разработать методы и средства оценки эффективности реализации функциональных и гарантийных требований безопасности продуктов и систем информационных технологий» (шифр «Сервис»).

Принятие в 1999 г. нового международного стандарта ISO/IEC 15408, который получил название Общие критерии (ОК), послужило толчком к переходу исследований на новый уровень. Использование ОК в качестве методической базы обусловлено, прежде всего, их системностью и перспективностью. В настоящее время ОК представляют собой наиболее полный набор критериев безопасности ИТ, которые удовлетворяют потребностям заказчиков, разработчиков, испытателей и пользователей, определяют концепцию, функциональные и гарантийные требования безопасности. Функциональные и гарантийные требования жестко структурирова-

ны и регламентируют все этапы проектирования, разработки, испытания и эксплуатации объектов ИТ.

Создание нормативно-методической базы основывалось на разработке:

- основополагающих национальных стандартов [39–41];
- стандартов прикладного характера, базирующихся на документах первой группы [42, 43];
- документов, не являющихся нормативными, но необходимых при создании продуктов и систем информационных технологий, а также при их сертификационных испытаниях.

К таким документам относятся:

- профиль защиты корпоративной вычислительной сети, обрабатывающей служебную информацию ограниченного распространения и использующей открытые каналы передачи данных;
- профиль защиты корпоративной вычислительной сети, обрабатывающей служебную информацию ограниченного распространения и использующей защищенные каналы передачи данных;
- методика оценки качества профиля защиты продуктов и систем информационных технологий;
- методика оценки качества задания по обеспечению безопасности продуктов и систем информационных технологий;
- общая методика испытаний продуктов и систем информационных технологий на соответствие уровням гарантии.

Следует особо отметить участие лаборатории в создании картографического центра Минобороны Республики Беларусь, космической системы зондирования Земли и в выполнении программы «СКИФ». По указанным направлениям разработаны следующие документы:

- профиль защиты базовой конфигурации суперкомпьютерной системы кластерного уровня;
- положение по обеспечению безопасности информации, обрабатываемой суперкомпьютерным центром;
- профиль защиты интегрированного картографо-геодезического комплекса Минобороны Республики Беларусь;
- профиль защиты наземного сегмента космической системы зондирования Земли.

Результаты работы по программе «СКИФ» и созданию картографо-геодезического центра неоднократно докладывались на конференциях [44–48].

Перечисленные три группы документов охватывают практически все проблемные задачи, которые подлежат решению в области информационной безопасности.

Учитывая опыт специалистов института в решении различных задач информационной безопасности, начиная с 2004 г. лаборатория проблем защиты информации ОИПИ НАН Беларуси начала подготовку к проведению сертификационных испытаний. Но это уже четвертый этап истории развития проблемы.

4. Аттестация и сертификационные испытания

В настоящее время лаборатория проблем защиты информации завершила мероприятия по аккредитации лаборатории в качестве испытательной. Государственный стандарт Республики Беларусь своим решением от 1 ноября 2004 г. подтвердил, что испытательная лаборатория проблем защиты информации соответствует критериям системы аккредитации Республики Беларусь и аккредитована на техническую компетентность в соответствии с требованиями СТБ ИСО/МЭК 17025.

Область аккредитации охватывает:

- оценку безопасности продуктов и систем информационных технологий на соответствие уровням гарантии оценки 1 и 2 (УГО1 и УГО2);
- оценку качества профиля защиты продуктов и систем информационных технологий;
- оценку качества задания по безопасности продуктов и систем информационных технологий.

Заключение

Лаборатория проблем защиты информации прошла сложный путь становления и развития начиная с разработки концепций безопасности и кончая обоснованием требований безопасности к суперкомпьютерному центру коллективного пользования. Планы дальнейшего развития исследований по проблемам информационной безопасности содержат более глубокую проработку теоретических основ оценки эффективности защиты информационных систем; создание системы обнаружения атак, включающей подсистему поддержки принятия решения с использованием методов искусственного интеллекта; разработку нормативно-методических документов для типовых и конкретных информационных систем, а также проведение сертификационных испытаний продуктов и систем информационных технологий.

Список литературы

1. International standard ISO/IEC 15408–1, 2, 3 Information Technology – Security techniques – Evaluation Criteria for IT security. Part 1: Introduction and general model. Part 2: Security functional requirements. Part 3: Security assurance requirements.

2. Анищенко В.В., Фисенко В.К. Концепция информационной безопасности // Известия Белорусской инженерной академии. – 1997. – № 1. – С. 9-14.

3. Компьютерная преступность и информационная безопасность / Под общ. ред. А.П. Леонова. – Мн.: АРИЛ, 2000. – 552 с.

4. Анищенко В.В. Оценка информационной безопасности // Компьютер сегодня. – № 2. – 2000. – С. 103-108.

5. Анищенко В.В. Направления совершенствования нормативно-методической базы информационной безопасности банковских технологий // Безопасность информационных технологий. – М.: МИФИ, 1997. – Вып. 4. – С. 62-70.

6. Анищенко В.В. Нормативный аспект создания интегрированных систем безопасности в кредитно-финансовой сфере // Управление защитой информации. – 1997. – Т. 1. – № 2. – С. 77-81.

7. Анищенко В.В. К вопросу разработки профиля защиты банковского функционального класса информационной безопасности // Управление защитой информации. – 1998. – Т. 2. – № 1. – С. 58-59.

8. Анищенко В.В. Нормативно-методическая база информационной безопасности банковских технологий // Системы безопасности связи и телекоммуникаций. – М.: Гротек, 1998. – № 8. – С. 92-96.

9. Анищенко В.В., Вензель Е.Ф. Эффективность защиты информационных систем // Управление защитой информации. – 1998. – Т. 2. – № 2. – С. 129-130.

10. Анищенко В.В., Вензель Е.Ф., Томина Г.Д. Динамическая модель оценки эффективности защиты продуктов и систем информационных технологий // Автоматика и вычислительная техника. – Рига, 1999. – № 2. – С. 42-50.

11. Анищенко В.В. Общая характеристика международного стандарта ИСО/МЭК 15408–1,2,3 // Управление защитой информации. – 2001. – Т. 5. – № 2. – С. 187-194.

12. Анищенко В.В., Криштофик А.М. Экономические вопросы проектирования и разработки средств обеспечения безопасности активов // Комплексная защита информации: Сб. мат. VIII Междунар. конф., 23–26 марта 2004 г., Валдай, Россия. – Мн., 2004. – С. 16-19.

13. Анищенко В.В., Криштофик А.М. Базовая модель системы защиты активов объекта информационных технологий // Докл. Белорусского государственного университета информатики и радиоэлектроники: Мат. II Российско-белорусской науч.-техн. конф. «Технические средства защиты информации», 17-21 мая 2004 г., Нарочь, Беларусь. – Мн.: УП «Бестпринт», 2004. – № 5. – С. 9.

14. Анищенко В.В. Методологические основы сертификации средств защиты информации по требованиям информационной безопасности // Управление защитой информации. – 1997. – Т. 1. – № 1. – С. 26-34.

15. Анищенко В.В., Фисенко В.К. Процедуры и требования по взаимному признанию сертификатов в области безопасности информационных технологий // Управление защитой информации. – 2002. – Т. 6. – № 4. – С. 430-431.

16. Анищенко В.В., Фисенко В.К., Талалуева М.А. Типовые программа и методики аттестации объекта информатизации на информационную безопасность // Управление защитой информации. – 1998. – Т. 2. – № 1. – С. 55-57.

17. Анищенко В.В., Фисенко В.К. Категорирование объектов информатизации с использованием метода кластерного анализа // Тез. докл. 6-й Междунар. науч.-практ. конф. «Безопасность и защита информации сетевых технологий. Common Criteria». – СПб., 2001. – С. 21-23.

18. Анищенко В.В., Вервейко Б.М., Стецюренко В.И. К вопросу о методологии обнаружения аномальной сетевой активности для обеспечения защиты систем информационных технологий // Комплексная защита информации: Сб. мат. VIII Междунар. конф., 23–26 марта 2004 г., Валдай, Россия. – Мн., 2004. – С. 9-12.

19. К вопросу выявления аномальной активности на основе экспертных знаний / В.В. Анищенко, Ю.В. Земцов, Е.П. Максимович, В.К. Фисенко // Комплексная защита информации: Сб. мат. VIII Междунар. конф., 23–26 марта 2004 г., Валдай, Россия. – Мн., 2004. – С. 13-15.

20. Анищенко В.В., Земцов Ю.В. Система моделирования удаленных атак на компьютерные сети // Докл. Белорусского государственного университета информатики и радиоэлектроники: Мат. II Российско-белорусской науч.-техн. конф. «Технические средства защиты информации», 17–21 мая 2004 г., Нарочь, Беларусь. – Мн.: УП «Бестпринт». – № 5. – 2004. – С. 13-14.

21. Анищенко В.В., Земцов Ю.В. Обнаружение атак с помощью нечетких методов автоматической классификации // Мат. XII Общероссийской науч.-техн. конф. «Методы и технические средства обеспечения безопасности информации», 4–5 октября 2004 г., Санкт–Петербург. – СПб.: Изд-во Политехн. ун-та, 2004. – С. 84.

22. Анищенко В.В., Талалуева М.А., Фисенко В.К. Перспективы стандартизации в области безопасности информационных технологий // Управление защитой информации. – 2000. – Т 4. – № 3. – С. 337-341.

23. Анищенко В.В., Фисенко В.К. Опыт работы по внедрению в Беларуси международных стандартов ИСО/МЭК 15408 «Критерии оценки безопасности информационных технологий» // Мат. Междунар. науч.-техн. конф. «Стандартизация. Сертификация. Качество», 27–28 ноября 2003 г., Минск. – Мн.: БелГИСС, 2003. – С. 108-110.

24. Анищенко В.В., Фисенко В.К. Профили защиты. Состояние и перспективы их разработки в Республике Беларусь // Тез. докл. 6-й Междунар. науч.-практ. конф. «Безопасность и защита информации сетевых технологий. Common Criteria». – СПб., 2001. – С. 23-25.

25. Качан О.А., Фисенко В.К. О регистрации профилей защиты продуктов и систем информационных технологий и создании государственного регистра // Докл. Белорусского государственного университета информатики и радиоэлектроники: мат. II Российско-белорусской науч.-техн. конф. «Технические средства защиты информации», 17–21 мая 2004 г., Нарочь, Беларусь. – Мн.: УП «Бестпринт». – № 5. – 2004. – С. 14.

26. Талалуева М.А., Фисенко В.К. Показатели оценки качества задания по обеспечению безопасности информационных технологий // Известия Белорусской инженерной академии. Спец. вып.: Мат. 6-й Междунар. науч.-техн. конф. «Современные средства связи». – Мн., 2001. – № 1 (11)/2. – С. 116-119.

27. Анищенко В.В., Стецюренко В.И. Концепция безопасности корпоративных ИВС на основе межсетевых экранов и профиля их защиты на базе Общих критериев // Известия Белорусской инженерной академии. Спец. вып.: Мат. 2-й Междунар. науч.-техн. конф. «Современные средства связи». – Мн., 1997. – № 1 (3)/2. – С. 15-18.

28. Анищенко В.В., Стецюренко В.И., Батраков А.Г. Перспективы совершенствования технологии создания и оценки защитных свойств межсетевых экранов на основе Общих критериев // Управление защитой информации. – 1998. – Т. 2. – № 1. – С. 39-41.

29. Анищенко В.В., Стецюренко В.И. Межсетевые экраны. Классификация, общие требования и их соответствие Общим критериям // Известия Белорусской инженерной академии.

Спец. вып.: Мат. 6-й Междунар. науч.-техн. конф. «Современные средства связи». – Мн., 2001. – № 1 (11)/2. – С. 125-127.

30. Стецюренко В.И., Батраков А.Г. Концепция «Положения по информационной безопасности корпоративных ИВС при взаимодействии с Internet» // Комплексная защита информации: Сб. науч. тр. Вып.2. – Мн.: Ин-т техн. кибернетики НАН Беларуси, 1999. – С. 85-94.

31. Анищенко В.В., Шаренков А.В., Федулов А.В. Система обнаружения удаленных сетевых атак «Мониторинг-LN» // Мат. IV Междунар. конф. «Комплексная защита информации», 29 февраля – 2 марта 2000 г., Раубичи. – Мн.: Ин-т техн. кибернентики НАН Беларуси, 2000. – С. 54-55.

32. Анищенко В.В., Стежко И.К., Тепляков А.А. Проблемы создания устройств защиты информации персональных электронных вычислительных машин от несанкционированного доступа // Мат. IV Междунар. конф. «Комплексная защита информации», 29 февраля – 2 марта 2000 г., Раубичи. – Мн.: Ин-т техн. кибернентики НАН Беларуси, 2000. – С. 49-50.

33. Анищенко В.В., Стежко И.К., Тепляков А.А. Аппаратно-программный комплекс средств защиты информации от несанкционированного доступа с применением средств криптографии // Комплексная защита информации: Сб. науч. тр. Вып. 3. – Мн.: Ин-т техн. кибернетики НАН Беларуси, 2000. – С. 118-124.

34. Вензель Е.Ф., Томина Г.Д. Критерии качества и оценки защиты сетевых ресурсов // Комплексная защита информации: проблемы и решения: Мат I Республ. науч.-практ. конф. – Мн., 1997. – С. 19-21.

35. Анищенко В.В., Надольский И.А. Средства автоматизированного формирования функциональных требований безопасности профилей защиты // Управление защитой информации. – 1998. – Т. 2. – № 1. – С. 36-38.

36. Анищенко В.В. Требования к автоматизированным средствам разработки профилей защиты // Управление защитой информации. – 1998. – Т. 2. – № 1. – С. 33-36.

37. Anishchenko V.V., Venzel E.F., Tomina G.D. A dynamic model for evaluation of the information technology product and system protection efficiency // Automatic Control and Computer Sciences. – V. 33. – № 2. – 1999. – P. 35-42.

38. Надольский И.А. Автоматизация процесса формирования требований безопасности к системам информационных технологий // Комплексная защита информации: Сб. науч. тр. Вып. 3. – Мн.: Ин-т техн. кибернетики НАН Беларуси, 2000. – С. 60-67.

39. СТБ 34.101.1,2,3–2004 (ИСО/МЭК 15408–1,2,3-99). Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1: Введение и общая модель; Часть 2: Функциональные требования безопасности; Часть 3: Гарантийные требования безопасности.

40. СТБ П 34.101.5–2003. Информационная технология и безопасность. Общая методология испытаний продуктов и систем информационных технологий на соответствие уровням гарантии.

41. СТБ П ИСО/МЭК 17799–2000/2003. Информационная технология и безопасность. Правила управления информационной безопасностью.

42. СТБ П 34.101.6–2003. Информационная технология и безопасность. Задание по обеспечению безопасности. Разработка, обоснование, оценка.

43. СТБ П 34.101.7–2003. Информационная технология и безопасность. Профиль защиты. Разработка, обоснование, оценка.

44. Анищенко В.В., Земцов Ю.В. Обнаружение атак на суперкомпьютерные системы // Тез. докл. Междунар. конф. «Суперкомпьютерные системы и их применение. SSA'2004». – Мн.: ОИПИ НАН Беларуси, 2004. – С. 227-232.

45. Анищенко В.В., Криштофик А.М. Разработка функциональных требований безопасности к высокопроизводительным вычислительным системам на основе анализа рисков // Тез. докл. Междунар. конф. «Суперкомпьютерные системы и их применение. SSA'2004». – Мн.: ОИПИ НАН Беларуси, 2004. – С. 238-243.

46. Анищенко В.В., Криштофик А.М. Методика оценки защищенности объектов информационных технологий при повышенных требованиях безопасности // Тез. докл. VI Военно-науч. конф. Военной академии Республики Беларусь, 25–26 ноября 2003 г. – Мн.: ВА РБ. – С. 198-200.

47. Мартинович Т.С., Талалуева М.А. Вопросы безопасности информации суперкомпьютерного центра Беларуси // Комплексная защита информации: Сб. мат. VIII Междунар. конф., 23–26 марта 2004 г., Валдай, Россия. – Мн., 2004. – С. 158-160.

48. Турбин С.К., Фисенко В.К. Пакеты функциональных требований по защите информации от несанкционированного доступа для типового картографического центра // Комплексная защита информации: Сб. мат. VIII Междунар. конф., 23–26 марта 2004 г., Валдай, Россия. – Мн., 2004. – С. 163-165.

Поступила

Объединенный институт проблем
информатики НАН Беларуси,
Минск, Сурганова, 6
e-mail: fisenko@newman.bas-net.by

Anishchanka U.V., Fisenka U.K.

FROM THE CONCEPT OF INFORMATION SECURITY UP TO THE SECURITY OF SUPERCOMPUTER SYSTEMS

The paper presents the results of analytical survey of main stages of formation and development of research in the field of information security in UIIP of NAS of Belarus.