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

Отмечается, что гармонизация – это согласование ПС и ФГОС по следующим основным параметрам:

1. Терминология;
2. Сроки действия;
3. Соотношение фундаментальности и практикоориентированности;
4. Оценка квалификаций.

По каждому из этих параметров дается сравнительная оценка ФГОС и ПС. В частности, отмечается несогласованность терминологии образовательных и профессиональных стандартов.

Нет также согласованности по срокам действия стандартов.

Большие трудности возникают и с независимой оценкой квалификаций.

Список литературы

1. ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата).
2. ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратуры).
3. ФГОС ВО по специальности 10.05.01 Компьютерная безопасность (уровень специалитет).
4. ФГОС ВО по специальности 10.05.02 Информационная безопасность телекоммуникационных систем (уровень специалитет).
5. ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (уровень специалитет).
6. ФГОС ВО по специальности 10.05.04 Информационно-аналитические системы безопасности (уровень специалитет).
7. ФГОС ВО по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере (уровень специалитет).
8. Специалист по безопасности компьютерных систем и сетей.
9. Специалист по защите информации в телекоммуникационных системах и сетях.
10. Специалист по защите информации в автоматизированных системах.
11. Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности.
12. Специалист по технической защите информации.

ОСНОВНЫЕ НАПРАВЛЕНИЯ ПО СОВЕРШЕНСТВОВАНИЮ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ БЕЛАРУСИ И РОССИИ

А.Г. СИЛИЦКИЙ

Оперативно-аналитический центр при Президенте Республики Беларусь

В целях обеспечения защиты общих информационных ресурсов Республики Беларусь и Российской Федерации осуществляется реализация программ Союзного государства.

В 2015 году завершено выполнение третьей программы «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на основе высоких технологий».

В результате выполнения 16 мероприятий (семь НИР и девять ОКР) белорусской стороной получено: 9 опытных образцов средств технической (криптографической) защиты информации, 3 программных продукта (специальное программное обеспечение), 36 проектов нормативно-правовых, методических, технических нормативных правовых документов.

Реализация программы позволила за пятилетний период получить приращение значений целевых индикаторов программы:

на 25% по возможностям средств обеспечения безопасности информации в критически важных системах информационной инфраструктуры по нейтрализации угроз безопасности информации с 12 до 37 процентов относительно требуемого количества подлежащих решению задач защиты информации;

на 31% по возможностям средств защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну (государственные секреты), по нейтрализации угроз безопасности информации за счет утечки информации по техническим каналам и несанкционированного доступа к информации с 25 до 56 процентов относительно требуемого количества подлежащих решению задач защиты информации.

В настоящее время проводятся процедуры по внедрению результатов программы. Разработаны предложения по направлениям дальнейших исследований до 2021 года в области совершенствования системы защиты информационных ресурсов Республики Беларусь и Российской Федерации.

Анализ показывает, что в период до 2021 года прогнозируется дальнейшее усиление противоборства государств в информационной сфере, использование террористическими и экстремистскими группировками новых методов информационных воздействий для достижения своих целей, увеличение количества компьютерных атак на информационные системы, в том числе информационные системы, обеспечивающие деятельность Союзного государства. При этом нарастание опасности угроз в информационной сфере в указанный период определяется следующими факторами:

появление новых методов и средств скрытного проникновения в информационные системы, расширение технических возможностей и навыков иностранных государств (специальных подразделений «центров киберкомандований»), преступных сообществ («хакерских группировок») и отдельных лиц («хакеров») по организации и проведению целенаправленных компьютерных атак на информационные системы, что приведет к существенному сокращению времени проникновения (от дней и часов до минут и секунд) в защищаемые информационные системы, обеспечивающие деятельность Союзного государства и государств-участников;

совершенствование системного, прикладного программного и программно-аппаратного обеспечения информационных систем с преимущественным использованием в них программных и программно-аппаратных средств зарубежного производства, что приведет к повышению эффективности недекларированных возможностей и скрытности проникновения в информационные системы, обеспечивающие деятельность Союзного государства и государств-участников;

интенсификация разработки иностранными государствами и преступными сообществами способов и средств несанкционированного доступа в информационные системы, прежде всего на основе применения высокотехнологичных многоплатформенных вредоносных программ, существенное расширение способов проведения сете-

вых атак на эти системы из сетей общего пользования путем создания нетрадиционных каналов доступа и воздействия, применения разнообразных приемов маскировки атак, таких как кодирование, сокрытие программного кода от исследований, переадресация, стеганография, «фишинг» (формирование ложных сообщений, в том числе содержащих вредоносные программы, в виде официальных писем) и др.;

внедрение новых информационных технологий (в том числе технологий виртуализации и «облачных» вычислений, технологий радиочастотной идентификации – RFID-технологий и т.д.) в информационные системы (в том числе банковские платежные системы, системы безопасности и охраны, медицинские системы, системы электронного документооборота, системы контроля за движением товаров и др.), что приводит к появлению новых уязвимостей и расширению спектра угроз безопасности информации, циркулирующей в информационных системах Союзного государства и государств-участников;

наращивание иностранными государствами, возможностей систем перехвата и обработки информации в информационных системах.

Перечисленные вопросы определяют актуальность проблемы постоянного совершенствования научно-технического и нормативно-методического обеспечения защиты информационных ресурсов Союзного государства и государств-участников. Данные угрозы безопасности информации существенно увеличивают объем и сложность задач по их предупреждению и нейтрализации.

В соответствии с Приоритетными направлениями и первоочередными задачами дальнейшего развития Союзного государства на среднесрочную перспективу (2014 – 2017 годы) ФСТЭК России совместно с ФСБ России и Оперативно-аналитическим центром при Президенте Республики Беларусь разработан проект Концепции программы Союзного государства «Совершенствование системы защиты информационных ресурсов Союзного государства и государств-участников Договора о создании Союзного государства в условиях нарастания угроз в информационной сфере» на 2017 – 2021 годы. Проект Концепции согласован уполномоченными органами Республики Беларусь и проходит согласование в Российской Федерации.

В Концепции определены следующие основные направления деятельности в области защиты информации и обеспечения бесперебойного функционирования критически важных объектов с учетом актуальных и появившихся новых угроз безопасности в информационной сфере:

выявление уязвимостей системного и прикладного программного обеспечения, используемого в информационных системах Союзного государства и государств-участников, в автоматизированных системах управления технологическими процессами критически важных объектов Республики Беларусь и Российской Федерации и разработку описательных моделей угроз безопасности информации;

разработка перспективных способов, методов и средств защиты информации на основе применения новых технологий (в том числе технологий виртуализации, «облачных» вычислений, элементов искусственного интеллекта, использования новых криптографических методов и аппаратных средств), разработка новых технологий защиты информации от несанкционированного доступа и от её утечки по техническим каналам, средств обнаружения компьютерных атак;

развитие методического обеспечения организации защиты и построения систем защиты информации в информационных системах государств-участников, развитие методического обеспечения мониторинга и прогнозирования угроз безопасности информации в информационных системах, подключенных к сетям общего пользования.

В рамках новой программы белорусской стороной запланировано выполнение следующих мероприятий:

выявление уязвимостей автоматизированных систем управления критически важных объектов, разработка моделей угроз и механизмов защиты информационных ресурсов;

разработка программно-аппаратного комплекса обнаружения аномалий в сетевом потоке автоматизированных систем управления критически важных объектов;

создание программно-аппаратного комплекса для выявления специальных технических средств негласного получения информации, передающих информацию по сетям сотовой связи;

создание средств оценки информационной инфраструктуры операторов электросвязи на предмет присутствия вредоносного воздействия;

разработка средств поиска в программном обеспечении недекларированных возможностей (скрытого и/или не описанного функционала, ошибок);

разработка программного комплекса регистрационного центра инфраструктуры открытых ключей на основе WEB-технологий в «облачном сервисе», программного комплекса мониторинга событий безопасности информационных систем инфраструктуры открытых ключей;

разработка программно-аппаратного средства канального шифрования на мобильных устройствах;

разработка новых криптографических стандартов и методик испытаний средств криптографической защиты информации, создание программно-аппаратного комплекса тестирования критических элементов инфраструктуры открытых ключей.

Государственными заказчиками программы прогнозируется, что результаты запланированных научно-исследовательских и опытно-конструкторских работ за очередной пятилетний период с 2017 по 2021 год позволят получить приращение значений целевых индикаторов программы до 61 процента по возможностям средств обеспечения безопасности информации в критически важных системах информационной инфраструктуры и до 83 процентов по возможностям средств защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну (государственные секреты).

Внедрение результатов, полученных в рамках программ Союзного государства, и реализация новых программных мероприятий позволит получить положительный экономический эффект для Беларуси и России за счёт:

предотвращения возможного ущерба при нарушении функционирования информационно-телекоммуникационных систем органов власти и организаций Союзного государства или минимизации такого ущерба в случае реализации информационных угроз;

экономии расходов Беларуси и России на защиту национальных информационных ресурсов и обеспечение безопасности информации в критически важных системах информационной инфраструктуры в результате применения средств защиты информации, единых нормативных правовых и методических документов;

сохранения научно-технического потенциала в области защиты информации, развития производства конкурентоспособных технических, программно-аппаратных и программных средств защиты информации.

На данном этапе основной проблемой является длительная процедура согласования в Российской Федерации проекта Концепции программы Союзного государства, что может привести к переносу срока начала выполнения программы на 2018 год.