Технические науки

УДК 004.056

Сезонова Ирина Константиновна
кандидат технических наук, доцент, заведующий кафедры
информационной и экономической безопасности
Харьковский национальный университет внутренних дел

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ ГОСУДАРСТВЕННОГО ПОДЧИНЕНИЯ
INFORMATION SECURITY COMPUTER SYSTEMS OF STATE SUBORDINATION

Аннотация: задача построения эффективной системы информационной безопасности решается с использованием системного и проектного подходов, которые, не только полностью учитывают типизацию объектов информатизации, но и позволяют трансформировать систему при возникновении новых угроз или при ее естественном «старении».

Ключевые слова: информационная безопасность, несанкционированный доступ, государственные органы.

Summary: the problem of constructing an effective information security system is solved with the use of the system and the project approach, which not only fully take into account the types of objects informatization, but also allow transforming system in the event of new threats or her aging.

Key words: information security, unauthorized access, the authorities.

Информационная безопасность (ИБ) является неотъемлемой составляющей национальной безопасности государства. Решение задачи обеспечения ИБ является комплексной и многозадачной проблемой,

решение которой нужно начинать на этапе проектирования компьютерной системы и заканчивать на этапе завершения ее работы (на современном этапе – замены на новую, более совершенную).

Современные информационно-регистрационные и компьютерные справочные системы государственного подчинения фиксируют и сохраняют информацию, которая может быть объектом несанкционированного доступа (НСД) с целью ее изменения, изъятия или использования в корыстных (или в преступных) целях. Особенно это касается правоохранительных органов и органов безопасности, которые должны не только обеспечить накопление, но и сохранение информации государственно-управленческого характера, а также быть готовыми к борьбе с новой категорией преступлений – киберпреступлениями, т.е. к правонарушениям в сфере информационных технологий.

Анализ последних публикаций показал, что научные исследования по решению указанной проблемы проводятся достаточно интенсивно. Публикации А.С.Гринберга, Н.Н. Горбачева, А.А. Теплякова, А.С. Маркова, С.В. Миронова, В.Л. Цирлова, Д.Н. Шакина, Р.М. Юсупова и др. посвящены разработке основ ИБ, законодательно-правовым, программно-техническим и организационным средствам ее обеспечения. Однако, проблема разработки методологии защиты информации, которая является собственностью государства, и способов оценки эффективности этой защиты, в научной литературе не встречаются. Стоит отметить, что несмотря на активные исследования проблемы оценки эффективности состояния защиты, в трудах ученых уделяется недостаточное внимания вопросу изучения и определения подходов к решению данной проблемы. Поэтому установление подходов к оценке эффективности состояния защиты требует дополнительных научных исследований.

Известно, что современные информационные технологии, в том числе и высокоэффективные технические средства, с помощью которых

можно легко получать, пересылать и анализировать информацию, позволяют иностранным государствам реализовать собственные интересы без применения военной силы, ослабить или нанести значительный ущерб безопасности страны. Вместе с тем, на фоне общего динамичного развития систем ИБ, интенсивной гармонизации национальной нормативной базы с мировыми и европейскими стандартами в области защиты информации ситуация выглядит стабильно консервативной, отстраненной по восприятию и использованию новых направлений, технологий и идей.

К предметным областям, которые нуждаются в строго научной и эффективной разработке концепции, методологии, алгоритмов и правил ИБ можно отнести: правоохранительные органы, органы государственной безопасности, судебные и налоговые органы, таможенные службы, медицинские организации, органы лицензирования и регистрации прав и др.

Решения задачи разработки системы ИБ начинается с анализа и характеристики угроз. Характеристика угроз существенно зависят от видов и типов информационно-телекоммуникационных систем, их пространственного размещения, степени взаимной совместимости, что усложняет процедуру определения их формального перечня. Проблема обеспечения эффективной защиты информации в случае государственных структур всегда регламентируется жесткими финансовыми условиями, которые также нужно учитывать при разработке концепции и методологии.

Рассмотрим организационно-методический и правовой аспект проблемы создания системы ИБ. Ситуация в этом аспекте характеризуется пока бессистемным развитием украинского законодательства, регулирующего отношения в информационной сфере с опозданием во времени (ориентировочно на 5-20 лет относительно времени издания аналогичных законодательных актов в других странах). Рассмотрев

структуру закрепления действующими нормативно-правовыми актами правовых норм по защите информации, можно прийти к выводу, что они по совокупности не позволяют решать проблемы методического обеспечения защиты информации и ИБ государства во всех их составляющих [1]. Существует довольно распространенное мнение о невозможности (или несоответствии по этическим соображениям) использования денежного измерения для определения убытков (вреда), возникшие в результате нарушения ИБ. Применение условных балльных оценок (расчетных или экспертных) вреда, причиненного полной или частичной потерей информации, в определенной степени позволяет снять этот проблемный аспект. Обратная процедура определения ущерба от потери информации по ее условно-бальной оценке позволяет рассчитать возможный вред от потери этой информации вследствие реализации той или иной угрозы.

Создание или модернизация информационных ресурсов государственного подчинения включает весь комплекс средств и мер ИБ. Для успешного выполнения поставленной задачи проектировщик и заказчик должны действовать по определенному алгоритму, который начинается с предпроектной стадии и заканчивается актом приема системы ИБ в эксплуатацию после соответствующих испытаний.

На предпроектной стадии система защиты информации определяется на общем, концептуальном уровне для того, чтобы правильно определить основные приоритеты ее построения и взаимосвязь между ее отдельными компонентами.

Предпроектная стадия включает:

1) определение перечня сведений, подлежащих защите от НСД и от утечки информации по техническим каналам;

2) проведение анализа территориального расположения и режима функционирования объекта защиты;

3) проведение анализа организации физической охраны, пропускного и внутреннего режимов работы объекта защиты;

4) определения перечня помещений, подлежащих защите;

5) определение условий размещения объектов информатизации относительно периметра критических угроз;

6) проведение анализа организационной структуры объекта защиты;

7) проведение анализа ответственности персонала за обеспечение информационной безопасности;

8) определение режимов обработки информации, характеристик и класса защищенности компьютерных систем;

9) определение мер по обеспечению конфиденциальности информации в процессе проектирования объекта информатизации.

Предпроектное обследование защищаемого объекта проводится комиссией, назначенной руководителем государственного органа или специализированной сторонней организацией, которая имеет соответствующую лицензию.

Результатом предпроектного обследования должно быть аналитическое обоснование требований к системе ИБ, которое оформляется в виде пояснительной записки со следующими сведениями:

1) перечнем критических данных, т.е. информационных ресурсов, которые могут быть объектом НСД с указанием их уровня конфиденциальности и/или условно-бальной оценки;

2) перечнем сотрудников организации, которые имеют доступ к критических данных, с указанием их режима доступа;

3) матрицей доступа к критическим данных (которая представляет собой специфический инструмент для проектирования системы ИБ);

4) информационной характеристикой и оптимальной организационной структурой компьютерной системы, подлежащей защите;

5) перечнем объектов информатизации, которые подлежат защите;

6) перечнем помещений и технических средств, подлежащих защите;

7) матрицей моделей вероятного нарушителя системы защиты (человеческий фактор);

8) матрицей моделей вероятных угроз НСД;

9) перечнем технических каналов утечки информации, которые подлежат закрытию при выявлении НСД;

10) требованиями и возможностями по контролю эффективности работы системы ИБ.

На основании предпроектного обследования оформляется техническое задание на проектирование системы защиты, которое проходит согласование с проектной организацией, службой безопасности организации - заказчика и утверждается руководителем организации – заказчика.

Проект системы ИБ государственного органа включает разработку организационных и технических мероприятий политики информационной безопасности организаии, которая в свою очередь предполагает несколько уровней детализации.

Уровень «Организационная безопасность» включает: управление политикой ИБ; распределение обязанностей по обеспечению ИБ; регламентацию процесса обработки критических данных; мониторинг ИБ; регламентацию работы со сторонними организациями.

Уровень «Управление персоналом» включает: подбор персонала; включение вопросов ИБ в должностные обязанности сотрудников; обучение персонала; административное реагирования на инциденты нарушения ИБ.

Уровень «Физическая защита и защита от воздействий окружающей среды» включает: обеспечение безопасности и контроль доступа в зоны, которые охраняются; расположение и защита технического оборудования; обеспечение защиты электропитания и безопасности кабельной сети от

повреждения и перехвата информации; организация технического обслуживания оборудования.

Уровень «Безопасное администрирование систем и сетей» включает: процедуры контроля действий системных администраторов на уровне операционной системы; защита от вредоносного программного обеспечения; порядок копирования и резервирования информации; управление безопасностью сети и ее мониторинг.

Уровень «Управления контролем доступа пользователя» включает: управление контролем доступа пользователя; контроль сетевого доступа; контроль доступа к операционной системе; контроль доступа к приложениям; мониторинг доступа и использования системы.

Ввод в эксплуатацию системы защиты сопровождается:

1) проведением опытной эксплуатации в комплексе с другими техническими и программными средствами с целью проверки ее работоспособности и отработки технологического процесса обработки (передачи) информации;

2) проведением испытаний системы защиты с искусственным моделированием различных видов НСД;

3) проведением оценки защищенности объекта информатизации и ее соответствие требованиям ИБ.

По окончании всех стадий создаются и утверждаются акты внедрения и акты соответствия объектов информатизации требованиям ИБ.

Одним из важнейших организационных моментов создания системы ИБ является необходимость размежевания исполнителей различных этапов, т.е. проведение различных этапов работ нужно поручать разным организациям. Этап предпроектного обследования и его аналитического обоснования выполняется заказчиком или его представителем. Для выполнения работ по созданию системы защиты необходимо привлекать

специализированные организации, имеющие необходимые лицензии на право проведения работ по защите информации и др. Техническое сопровождение, включая мониторинг ИБ, необходимо осуществлять силами организации-заказчика, желательно с использование отдельной службы.

Управление и проектирование систем ИБ неэффективно без внедрения современных информационных технологий и достижений математических, кибернетических, управленческих наук. Только современные информационно-технические средства и методы помогают обеспечить необходимые принципы защиты информации при проектировании и эксплуатации информационно-компьютерных систем.

Результативность анализа и полнота обработки все возрастающих объемов открытой информации, которая является собственностью государства, и информации с ограниченным доступом (конфиденциальной и секретной), требование относительно защиты которой установлено законом, возможны только в условиях применения различных информационно-коммуникационных технологий и общегосударственных информационно-аналитических систем различного уровня и назначения.

В статье для решения задачи построения эффективной системы ИБ предложено использовать системный и проектный подходы, которые, в отличие от существующих, полностью учитывают все виды объектов информатизации, позволяют трансформировать систему ИБ при возникновении новых угроз или при ее естественном «старении». Правовые нормы по обеспечению защиты информации на доктринальном, концептуальном, стратегическом, программном и плановом уровнях на сегодня фактически не имеют достаточного законодательного закрепления и потому, требуют комплексного изучения и усовершенствования.

Литература:

1. *Доктрина інформаційної безпеки України : Указ Президента України від 8 лип. 2009 р. № 514/2009 // Офіц. вісн. України. - 2009. - № 52. - Ст. 1783.*

2. Гринберг А.С. Защита информационных ресурсов государственного управления / А. С. Гринберг, Н. Н. Горбачев, А. А. Тепляков. - М. : ЮНИТА-ДАНА, 2003. - 327 с.

3.Марков А.С. Разработка политики безопасности организации в свете новейшей нормативной базы / А.С. Марков, С.В. Миронов, В.Л.Цирлов // Защита информации. Конфидент - 2004 - №2.

4. Юсупов Р.М. Наука и национальная безопасность. 2-е издание. СПб.: Наука, 2006.- 290 с.