определение взаимодействия организационных ролей в УК;

таблицы разрешенных действий для ролей при выполнении ими своих задач;

согласованные критерии выбора объектов конфигурации;

описание ресурсов, выделенных для УК;

инструментальные средства, применяемые для управления конфигурацией, их возможности и технические характеристики;

количество задействованного персонала, его квалификация;

порядок и периодичность создания версий и редакций продуктов;

схема взаимодействия с субподрядчиками, заказчиками при сопровождении продуктов.

3. Идентификация конфигурации:

определение элементов конфигурации;

определение системной архитектуры элемента конфигурации или дерева элементов конфигурации;

определение документов, которые должны контролироваться УК;

определение системы присвоения имен и идентификаторов элементов конфигурации.

4. Контроль конфигурации:

порядок запроса на изменение элементов конфигурации;

формат и структура запроса на изменения элемента конфигурации;

определение схемы оценки предлагаемых изменений элементов конфигурации;

определение схемы санкционирования (или отказа) изменения элементов конфигурации;

схема реализации изменений;

схема проверки реализованных изменений;

определение схемы маркировки запроса на изменение элемента конфигурации (при отклонении и одобрении).

5. Отчет о статусе конфигурации:

основные виды отчетов о статусе конфигурации;

определение частоты отчетности о статусе конфигурации.

6. Аудит конфигурации:

типы отчетов аудита и их периодичность.

А.П. Жалов

О БЕЗОПАСНОСТИ И СТОИМОСТИ ОПЕРАЦИОННЫХ СИСТЕМ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СРЕДСТВ КОМПЬЮТЕРНОЙ ТЕХНИКИ

Операционная система (ОС) представляет собой базовый набор функций, обеспечивающий управление аппаратными средствами компьютера. Существует большое количество ОС, но на настольных ком-

пьютерах наиболее часто встречаются ОС семейства Windows, следующими по популярности являются операционные системы семейства Linux.

Указанная ситуация определяется в первую очередь наличием большого количества программного обеспечения под ОС Windows (в основном игры), а также большим количеством платных программ для профессиональной деятельности (AutoCad, P-Cad, Coreldraw, 1СБухгалтерия) и других, предназначенных как для решения узкого круга профессиональных вопросов, так и для решения более общих задач. Следует заметить, что в последнее время ряд производителей программного обеспечения выпускают свои продукты как для Windows, так и для Linux.

Однако в составе ОС семейства Linux также есть бесплатные приложения, например программные продукты, позволяющие работать с текстовыми файлами формата *.doc (*.docx), с табличными файлами формата *.xls (*.xlsx), с файлами презентаций формата *.ppt (*.pptx), входящие в пакет OpenOffce. Таким образом, можно решать ряд вопросов, связанных с созданием различных документов в текстовой форме, табличной форме, а также создавать презентации, работать в интернете, просматривать файлы *.pdf, *.djvu, т. е. выполнять широкий перечень типовых офисных задач.

На тему безопасности дебаты идут практически со времен существования систем Windows и Linux. По этому поводу можно привести статистическую информацию, которая, правда, относится к web-серверам, но все же позволяет сделать вывод о безопасности операционных систем. Компания Netcraft регулярно проводит обзор web-сайтов. Так, на февраль 2010 г. 54,46 % web-сайтов используют web-сервер Apache, который работает под управлением ОС семейства Linux, и только 24,57 % используют web-сервер Microsoft IIS, работающий соответственно под управлением ОС Windows Server. Приведенные данные говорят о том, что для сервера предпочтительной является ОС семейства Linux. Думается, что это происходит из соображений безопасности данных, хранящихся на сервере, и устойчивости ОС в работе. Кроме того, впечатляет информация о заражении вирусами свежеустановленной версии Windows XP через 16 мин. после подключения компьютера к интернету. Времени, необходимого для загрузки и инсталляции программных продуктов, которые позволят защитить этот компьютер, требуется больше. Для ОС семейства Linux подобные сведения отсутствуют. Однако исходя из опыта использования данной ОС можно утверждать, что она устойчиво работает многие годы в интернете, не прибегая к помощи программ по защите.

Таким образом, помимо платных ОС от Microsoft семейства Windows существуют еще и бесплатные операционные системы, например

Linux. Для операционных систем Windows компанией Microsoft поставляется еще и платный продукт MicrosoftOffice, предоставляющий широкие возможности по работе с документами. Однако существуют и бесплатные программные продукты, возможности которых по работе с документами не уступают продуктам от Microsoft.

По вопросам безопасности бесплатные ОС семейства Linux не уступают платным ОС семейства Windows, правда, если на них установлено платное специальное ПО для защиты данных ОС от вредоносных программ.

Для выполнения большинства офисных задач достаточно использовать бесплатное программное обеспечение: операционную систему семейства Linux, входящий в нее пакет для работы с документами OpenOffice. Решение об установке на офисных компьютерах операционной системы семейства Linux позволит избежать игр подчиненных в рабочее время, так как подавляющее большинство игр создаются под операционную систему Windows и не могут работать под управлением операционных систем семейства Linux; снимет вопросы, связанные с приобретением лицензий на платные программные продукты; избавит от необходимости приобретения программных продуктов для защиты компьютера от вирусов и постоянного их обновления.

В.Ф. Картель

ЗАЩИТА КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ИНФРАСТРУКТУР КАК ФАКТОР ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ГОСУДАРСТВА В ИНФОРМАЦИОННОЙ СФЕРЕ

В настоящее время жизнь общества характеризуется динамичным развитием современных информационных технологий. Системы и средства вычислительной техники и современные телекоммуникационные сети являются неотъемлемой частью нашей жизни и одним из главных факторов, влияющим на все сферы жизни и развития общества.

В настоящее время информация является таким же богатством страны, как производственные и людские ресурсы. В современном мире, тяготеющем к глобализации и взаимопроникновению экономик, основанном на обмене новейшими научными достижениями, проблемы информационной безопасности приобретают особую актуальность.

От успешного решения вопросов безопасности и уровня защищенности информационной среды в сфере государственного управления, в различных отраслях промышленности, транспорта, в сфере торговли и

на финансовом рынке, во многом зависит конкурентоспособность белорусского государства и благополучие граждан.

Вместе с тем нельзя не отметить уязвимость информационных систем от широкого спектра угроз внешнего и внутреннего характера, а также высокую вероятность наступления серьезных негативных последствий, связанных с нарушением их функционирования.

Стремительное развитие информационных технологий и глобализация интернета в последнее десятилетие привели к тому, что элементы национальной критической инфраструктуры становятся объектом преступной деятельности; появляется больше «мишеней» для противоправных посягательств; террористические и криминальные группы получили возможность использования глобальной сети в своих преступных намерениях.

Высокая сложность и одновременно уязвимость всех систем, на которых базируются национальное, региональные и мировое информационные пространства, а также фундаментальная зависимость от их стабильного функционирования инфраструктур государства приводят к возникновению принципиально новых угроз. Эти угрозы связаны прежде всего с потенциальной возможностью использования информационно-телекоммуникационных инфраструктур в деструктивных целях.

Особая озабоченность в этом плане возникает в связи с разработкой, применением и распространением информационного оружия, в результате чего становятся возможны «информационные войны» и «информационный терроризм», основой которых является осуществление электронных, радиочастотных и компьютерных атак на критически важные объекты национальных информационно-телекоммуникационных инфраструктур (ИТИ), обеспечивающих управление в различных областях жизнедеятельности общества – государственного управления, обороны, экономики и т. д. Эти атаки имеют целью не только нанесение ущерба экономике страны. Их успешная реализация может привести к срыву задач государственного управления, в сфере обороны и управления войсками, оказанию психологического давления и возникновению паники среди населения и т. д.

Другим компонентом в списке основных угроз в информационной сфере следует назвать активизацию киберпреступности, основной целью которой являются не средства массовой информации и интернет, как это часто представляется в печати, а системы управления государством, экономикой, безопасности личности, манипулирования личным и общественным сознанием.

Мировая и отечественная статистика реализованных угроз в отношении объектов ИТИ, уязвимость современных информационно-теле-