один из своих пороков. Борджиа же был рожден властвовать, он был сыном своего времени, способным на все для достижения своей цели. Макиавелли, считавший Чезаре образцом монарха, охарактеризовал его так: «Герцог – человек, который более всех людей окружен тайной. Он не раскрывает ни одного своего намерения, пока его не осуществит».

Безспорно, фраза «Aut Caesar, aut nihil» отразилась на жизни и Калигулы и Борджиа. Первоначально служа оправданием пороков человекоподобного существа, волею судьбы получившего власть, она со временем трансформировалась, поменяв свой смысл и став жизненным кредом, линией поведения для неординарного и целеустремленного человека.

Литература

1. *Аксельрод А., Филлипс Ч.* Диктаторы и тираны. В 2-х тт.; Т 1/ Пер. с англ. В. Найденова, А. Марченко, Н. Дневой и др. Смоленск. Русич. 1998.
2. *Гончарова Н. А.* Из античной мудрости: Латинские пословицы и поговорки с русскими соответствиями. Мн. Выш. Шк., 2004.
3. *Овруцкий Н. О.* Крылатые латинские выражения в литературе.
4. *Рыжов К.* Все монархи мира. Древняя Греция, Древний Рим, Византия. М. Вече. 1998.
5. *Светоний.* Жизнь двенадцати Цезарей.

ЗАЩИТА ДОКУМЕНТАЛЬНОЙ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ И СЕТЯХ: ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЙ АСПЕКТ

О. Ю. Жук

Стремительное развитие информационных технологий открыло перед обществом широкие возможности по автоматизации труда и привело к созданию большого числа разного рода компьютерных систем и сетей, которые используются во всех сферах общественной жизни. Неправомерное искажение, фальсификация, уничтожение, разглашение информации, находящейся в этих системах и сетях, равно как и дезорганизация процессов ее обработки и передачи, наносят серьезный ущерб субъектам (государству, физическим и юридическим лицам), участвующим в процессах информатизации.

Результаты проведенных опросов показывают, что среди основных угроз безопасности 43 % составляют вирусы, 26 % – отказ в работе корпоративных систем, 15 % – атаки с целью вызвать отказ в обслуживании, 14 % – проникновение извне, 11 % – проникновение изнутри, 5 % – нарушение целостности данных, 3 % – финансовое мошенничество, 2 % – хищение коммерческой информации [9]. Средний ущерб от различных

типов атак на системы безопасности составляет: воровство данных компаний – 2 809 000 $, кража персональных данных – 1 677 000 $, саботаж – 86 000 $, мошенничество в области связи – 539 000 $, проникновение в систему из вне – 86 000 $, мошенничество в области финансов – 388 000 $ [1].

Защита документальной информации на сегодняшний день является одним из приоритетных направлений в деятельности компаний компьютерной индустрии и является важным направлением работы любой организации, которая использует в своей деятельности информационные технологии. Причем, это не односторонняя проблема, а сложный комплекс организационных и технических мероприятий, проводимых в целях сохранения от несанкционированного доступа интеллектуальной собственности каждого пользователя.

Организационно-технические меры являются важной составляющей всей системы защиты. Рассматривая этот аспект, выделяют технические и организационные меры защиты.

Технические меры основаны на использовании механических, электронно-механических устройств и специальных программ, входящих в состав компьютерной системы и выполняющих функции защиты (идентификация/аутентификация пользователей и ресурсов, разграничение доступа к ресурсам, регистрация событий, реагирование на попытки несанкционированного доступа и т. д.)

Основными техническими методами защиты являются препятствие и управление доступом, реализуемых на практике с помощью различных механизмов, для создания которых используются физические, аппаратные, программные средства (замки, микровыключатели, инерционные датчики, экранирующие и поглощающие материалы, жидко-кристаллические и плазменные дисплеи, струйные и термопринтеры, сетевые фильтры подавления электромагнитных излучений и т. д.) [5].

К мероприятиям по технической защите информации относятся идентификация/аутентификация участников информационного взаимодействия; защита технических средств от несанкционированного доступа; разграничение доступа к документам, ресурсам ЭВМ и сети; защита данных в каналах связи; разграничение доступа к потокам данных; защита информационных технологий [7].

Указанные методы и средства защиты, реализуются в продуктах, которые предлагаются на рынке информационных технологий. Например, система защиты информации от несанкционированного доступа «Криптон-вето» и комплекс «Криптон-замок», российской компании АНКАД [10]. Парольный доступ к персональному компьютеру обеспечива-

ют программы «Boot Locker», «PC Loc», «PGP Desktor Secrurity». Широкое применение нашли программы разграничения доступа «Assa» (г. Москва), «Ndmi» (г. Минск) [6]. На рынке СНГ представлены также биометрические системы контроля доступа по отпечаткам пальцев «Identix» (США) и биометрическая система контроля доступа по узору сетчатки глаза «Eyedetify». Среди систем разграничения доступа можно назвать и такие как «Net Ware», «Watch Doc», «Dallas Lock». Но необходимо сугубо осторожно относиться к любым сертификатам и отдавать предпочтение тем продуктам, надежность которых подтверждена успешным использованием в мировой практике [5]. Надежность и эффективность применения всех программных, аппаратных, криптографических средств защиты достигается только при выполнении определенных организационных мероприятий по защите информации.

По мнению зарубежных специалистов, организационные меры защиты, несмотря на постоянное совершенствование технических средств, составляют значительную часть (50 %) системы защиты [8]. Они используются тогда, когда компьютерная система не может непосредственно контролировать использование информации, и при дублировании технических мер в целях повышения степени защиты.

Организационные меры – это меры, регулирующие процесс функционирования системы обработки данных, использования ее ресурсов, деятельности пользователей таким образом, чтобы в наибольшей степени исключить возможность реализации угроз безопасности. Данные меры защиты охватывают процедуры и решения, принимаемые руководством организации – потребителем компьютерной системы. Часть из них определяется внешними факторами, например, законами. Большинство же проблем решается внутри организации в конкретных условиях.

Исследование показывает, что составной частью любого плана мероприятий является четкое указание целей, распределение ответственности и перечень организационных мер защиты. Конкретное распределение ответственности и функций по реализации защиты зависит от специфики деятельности организации, но тщательное планирование и точное распределение ответственности являются необходимым условием создания эффективной и жизнестойкой системы защиты.

В настоящее время существуют различные подходы в определении и классификации организационных мер защиты: на основе нормативно-технической, методической, организационно-распорядительной документации (В. Н. Везиров): перечень сведений конфиденциального характера, положение о порядке организации и проведении работ по защите информации, приказы о назначении лиц, ответственных за эксплуатацию

системы, технический паспорт на компьютерную систему и т. д.; на основе этапов жизненного цикла системы (В. В. Домарев): мероприятия, осуществляемые при создании информационной системы, при эксплуатации системы и мероприятия общего характера; по периодичности применения мер (В. Ю. Гайкович): разовые, проводимые при осуществлении или возникновении изменений в системе, периодически проводимые, постоянно проводимые [2; 4; 3].

Кроме того, важным аспектом является также организационная защита машинных носителей информации и мероприятия, проводимые при размещении, установке и функционировании средств защиты информации.

Выше перечисленные меры защиты отражаются в нормативно-методических документах службы безопасности, службы конфиденциального делопроизводства, должностных инструкциях работников данных подразделений.

Организационные меры играют значительную роль в обеспечении безопасности компьютерных систем. Это единственное, что остается, когда другие методы и средства защиты отсутствуют или не могут обеспечить требуемый уровень безопасности. Однако это вовсе не означает, что систему защиты необходимо строить исключительно на их основе, как это часто пытаются сделать чиновники далекие от технического прогресса. Этим мероприятиям присущи и серьезные недостатки: снижение надежности без соответствующей поддержки техническими, программными методами и средствами, дополнительные неудобства, связанные с большим объемом рутинной формальной деятельности.

Организационные меры являются основой, которая объединяет все остальные меры защиты в единую систему. Они необходимы для обеспечения эффективного применения других методов и средств защиты в части, касающейся регламентации действий людей. В тоже время эти меры необходимо поддерживать более надежными техническими средствами. Именно поэтому зачастую организационные и технические меры защиты рассматриваются в совокупности.

Выбор конкретного набора защиты зависит от специфики деятельности организации (структура, численный состав работников, объем конфиденциальной информации, материальная база и др.) и проводимой политики безопасности.

Литература

1. *Блек У.* Интернет: протоколы безопасности. Учебный кур с. СПб.: Питер, 2001. 288 с.

2. *Везиров В. Н.* Информационная безопасность и средства защиты информации в системе электронных закупок для государственных нужд // Вопросы защиты информации. М.: ГУП ВИМИ, 2003. №3 (62). С. 25–32.
3. *Гайкович В. Ю., Ершов Д. В.* Основы безопасности информационных технологий // http:www.kis-kiev.narod.ru. (10.04.2005).
4. *Домарев В. В.* Защита информации и безопасность компьютерных систем. К.: ДиаСофт, 1999. 480 с.
5. *Зубик В. Б.* Экономическая безопасность предприятия (фирмы). Мн.: Выш. шк., 1998. 391 с.
6. *Кауров Л. В.* Основы обеспечения безопасности информационных систем. М.: Институт управления и предпринимательства, 2002. 55 с.
7. *Конявский В. А.* Техническая защита электронных документов в компьютерных системах // Управление защитой информации. М–Мн., 2003. Том 7, №4. С. 10–16.
8. *Мельников В. В.* Защита информации в компьютерных системах. М.: Финансы и статистика, 1997. 368 с.
9. *Мур М.* Аналитическая поддержка безопасности информационных систем // Международный форум по информации. М.: ВИНТИ, 2002. Том 27, № 2. С. 36–43.
10. *Романец Ю. В., Тимофеев П. А.* Защита информации в компьютерных системах и сетях. М.: Радио и связь, 2001. 376 с.

НЕКАТОРЫЯ АСПЕКТЫ СТАНАЎЛЕННЯ НЕФАРМАЛЬНАГА РУХУ СЯРОД МАСТАКОЎ БЕЛАРУСІ

К. А. Луцкіна

Бурнае развіццё Беларусі напачатку 1990-х гадоў, імклівыя падзеі ў культурным жыцці, якія суправаджаліся распадам былых савецкіх творчых аб’яднанняў і ўзнікненнем на іх месцы новых, паставілі шэраг пытанняў аб вытоках дадзеных падзей. І калі развіццю палітычнага нефармальнага руху апошнім часам надавалася пэўная ўвага, то падзеі, звязаныя з развіццём падобных рухаў сярод творцаў альбо зусім не агучваліся, альбо далучаліся да ўжо вядомых палітычных груп, а такое паняцце як «андэграўнд» звычайна звязвалася з такімі буйнымі цэнтрамі як Масква, Ленінград і Вільнюс, а аб існаванні падобнага мастацтва ў іншых гарадах і рэспубліках Савецкага саюза было вядома даволі няшмат.

Адной з галоўных асаблівасцяў развіцця савецкага мастацтва ўвогуле было суіснаванне двух культур: так званых афіцыйнай і неафіцыйнай. Пры гэтым калі першую ўсяляк падтрымлівалі на самым высокім узроўні, то дзеля задушэння другой рабілася ўсё магчымае. На Беларусі неафіцыйнае мастацтва развівалася ў межах нефармальных груп і мела шэраг адрозненняў ад неафіцыйнага мастацтва, напрыклад, той жа Масквы. Сам тэрмін «нефармальнае аб’яднанне» ці «групоўка» ў навуковых і папулярных публікацыях звычайна ўжываецца разам з