1. Michel, J. B. Quantitative Analysis of Culture Using Millions of Digitized Books. Science / J. B. Michel [and other]. – 2010. – [Электронный ресурс]. – Режим доступа: https://books.google.com/ngrams/info. – Дата доступа: 25.05.2013.

2. Горный, Е. Проблемы сохранения культурного наследия в эпоху цифрового текста / Е. Горный. – 2012. – [Электронный ресурс]: Режим доступа: www.netslova.ru/gorny/digtext.html?2012. – Дата доступа: 24.05.2013.

3. Оцифровка книг позволит по-новому изучать историю и культуру [Электронный ресурс]. – Режим доступа: http://ria.ru/science/20101217/-309883432.html#13702723185043. – Дата доступа: 10.05.2013.

4. Google Books Ngram Viewer: What does the Ngram Viewer do? [Электронный ресурс]. – Режим доступа: https://books.google.com/ngrams/info. – Дата доступа: 20.05.2013.

5. Leetaru, K. H. Culturomics 2.0: Forecasting large-scale human behavior using global news media tone in time and space / K. H. Leetaru. – [Электронный ресурс]. – Режим доступа: https://books.google.com/ngrams/info. – Дата доступа: 18.10.2013.

А. Г. Зезюля,
доц. каф. информационных технологий в культуре БГУКИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УЧРЕЖДЕНИЯХ КУЛЬТУРЫ И ИСКУССТВ

Необходимость защиты информации осознавалась на протяжении всей истории развития человечества.

Особенно актуальной эта проблема стала в последние годы, которые характеризуются массовым использованием автоматизированных информационных систем в режиме интенсивного сетевого взаимодействия. Достижения современных компьютерных технологий в сфере обработки информации (сбора, хранения, поиска, преобразования, представления) предоставили новые возможности и существенные удобства. Результатом этого прогресса явилось то, что значительные объемы информации переведены и переводятся с традиционных носителей в виртуальную среду и процесс имеет ярко выраженную тенденцию. Значительная часть информации уже непосредственно функционирует только в виртуальном пространстве, а

традиционные носители используются только как архаичный способ донесения информации до потребителя.

В области художественной культуры и искусств использование компьютерных технологий приобретает особенно важное значение не только в качестве средства сохранения культурного наследия, продвижения всего многообразия артефактов мирового наследия в виртуальном пространстве, интенсификации взаимодействия национальных культур в глобальном масштабе, но и непосредственного использования компьютерных технологий в творческой деятельности, которое проявляется в создании новых жанров, видов, течений.

Термин «защита информации» в современной практике понимают в первую очередь как совокупность средств, методов, технологий, вовлеченных в непрерывный процесс обеспечения безопасности информации, которая функционирует в среде технической поддержки информационных коммуникаций и ресурсов.

Наиболее общей целью защиты информации как непрерывного процесса является обеспечение устойчивого и бесперебойного функционирования информации с соблюдением требований целостности, доступности и конфиденциальности.

Защита информации в учреждениях, предприятиях, организациях должна рассматриваться в тесной связи с решением задач защиты материальных и финансовых средств, обеспечением защиты от нарушений производственной деятельности, охраной здоровья и жизни персонала.

Однако планирование защиты информации не должно рассматриваться как сопутствующая задача. Защита информации на современном этапе является самостоятельной задачей в комплексе охраны законных интересов организации от противоправных посягательств.

Основой планирования систем защиты информации является создание концептуальной модели системы защиты информации, которая базируется на следующих основных принципах, применяемых для проектирования систем любой природы и сложности. Перечислим эти принципы.

1. Принцип системности, учет всех взаимосвязанных статических и динамических объектов (субъектов), условий и факторов, процессов информационной среды.

2. Принцип комплексности предполагает взаимосогласованное использование всех возможных разнородных средств и ме-

тодов защиты информации (в том числе и традиционных) в системе обеспечения информационной безопасности.

3. Принцип адекватности подразумевает использование соответствующих эффективных средств и методов защиты и своевременность их применения, а также адекватной и своевременной реакции системы.

4. Принцип непрерывности предполагает учет динамики в разработке средств проникновения и средств противодействия угрозам.

5. Принцип гибкости позволяет оперативно, без существенных изменений в структуре, перенастроить систему безопасности на эффективное противодействие угрозам в значительно изменившихся условиях функционирования.

6. Принцип прозрачности предполагает сокрытие деталей сложного механизма обеспечения безопасности информации с целью создания интуитивно понятной среды, которая не только не затрудняет, но более того способствует выполнению пользователем необходимых работ.

7. Принцип эффективности основан на создании оптимизированной, внутренне согласованной, эффективной системы противодействия угрозам и обеспечение безопасной работы с информацией.

8. Принцип унификации отражает необходимость создания стандартных сертифицированных средств и широкое их использование в системах безопасности.

9. Принцип собственной безопасности направлен на создание такой системы безопасности, которая обеспечивала бы эффективное противодействие даже в том случае, если бы нарушителю были бы известны структура, алгоритмы и средства противодействия угрозам. Этот принцип специфичен для систем безопасности информации. В литературе этот принцип иногда отождествляют с принципом открытости [1, 2].

10. Принцип согласованности. Внедрение комплексной системы безопасности изменяет информационную среду. В этой связи необходимо предусмотреть такие подходы к проектированию, которые бы предоставлями возможность обеспечения высокой степени информационной безопасности в измененной среде. Отметим, что в данном случае основой может служить системный подход.

При разработке концептуальной модели комплексной системы безопасности для учреждений культуры и искусств на

первом этапе необходимо определить состав информации, подлежащей защите. При этом весь объем информации следует разбить на определенные классы в зависимости от того, является ли информация строго конфиденциальной либо это требование к данной информации не предъявляется либо предъявляется в менее строгом смысле. Отметим, что в большинстве случаев для учреждений культуры и искусств проблема конфиденциальности затрагивает лишь коммерческую и персональную информацию, которые представляют небольшую часть всего объема информации. Более актуальной является проблема обеспечения целостности и сохранности информации, а также вопросы устойчивого и бесперебойного функционирования средств коммуникаций и соответствующих информационных ресурсов.

После выявления основного состава защищаемой информации необходимо определить источники, а также средства передачи и обработки информации. С этой целью производится изучение категорий пользователей и уязвимостей основных компонентов. Для решения этой задачи следует определить совокупность конкретных объектов защиты: информационные ресурсы, процессы обработки информации, а также иные объекты информационной инфраструктуры (технические и программные средства, средства коммуникаций, системы и средства защиты информации, условия функционирования).

Важное значение в создании эффективной системы защиты информации имеет изучение состава пользователей (конечных пользователей, администраторов информационных ресурсов, администраторов серверов, системных и прикладных программистов, разработчиков, специалистов по техническому обслуживанию, администраторов информационной безопасности), не только с целью разграничения прав доступа, но включения их в глубоко эшелонированную систему обеспечения безопасности путем перераспределения прав и делегирования полномочий для всех участников процесса функционирования и обеспечения безопасности информации.

Таким образом, надо отметить, что построение эффективных систем безопасности информации в настоящее время является весьма сложным процессом, который требует учета многих факторов и использования разнообразных средств защиты, функционирующих в комплексе.

Однако, анализируя основные требования к защите информации в учреждениях культуры, можно заключить о необходимости учета следующих базовых положений:

1. Планирование комплексной системы безопасности информации (КСБИ) должно осуществляться как самостоятельная задача.

2. Реализация КБСИ должна быть интегрирована в существующую информационную инфраструктуру и составлять с ней единое целое.

3. КБСИ должна рассматриваться как непрерывно развивающаяся система, которая формирует в упреждающем режиме эффективную безопасность информации.

Создание служб безопасности информации в учреждениях культуры и искусств низового звена не представляется экономически оправданным. Представляется более эффективным создание в рамках отрасли культуры отраслевого специализированного центра обеспечения безопасности информации, основной функцией которого являлась бы создание защищенной арендуемой платформы, предназначенной для размещения информационных ресурсов учреждений культуры республики, а также защищенных каналов связи (например, VPN) и обеспечение надежного обслуживания.

1. Биячуев, Т. А. Безопасность корпоративных сетей / под ред. Л. Г. Осовецкого. – СПб. : СПб ГУ ИТМО, 2004. – 161 с.

2. Грибунин, В. Г. Комплексная система защиты информации на предприятии : учеб. пособие для студ. высш. учеб. заведений / В. Г. Грибунин, В. В. Чудовский. – М. : Издательский центр «Академия», 2009. – 416 с.

Т. Д. Орешко,
ст. преп. каф. информационных технологий в культуре БГУКИ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ХУДОЖЕСТВЕННОЙ ДЕЯТЕЛЬНОСТИ

Современные информационные технологии оказывают влияние на все сферы жизни общества и отдельных индивидов.

Большое значение имеет использование информационных технологий в художественном творчестве и освоении культурного наследия.