Петров Сергей Томасович.
Москва, журнал «Цифровое наследие»,
сотрудник Музея-библиотеки Н.Ф. Федорова
Тел.: +7(495)500-86-04
E-mail: 5008604@gmail.com
Тарасов Александр Алексеевич.
Москва, Институт информационных наук и технологий безопасности РГГУ
Тел.: +7(495)388-08-88
E-mail: aa_tarasov@list.ru

УДК 004.056

С.Т. Петров, А.А.Тарасов

В статье рассматриваются проблемы информационной безопасности в сфере культуры. Описана методика комплексной оценки значимости культурных информационных активов. Представлен комплекс документов по рискам и угрозам информационной безопасности культуры.
Ключевые слова: информационные активы, цифровое наследие, культурные ценности, оценка значимости, оценка рисков, классы защищенности.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ АКТИВОВ В СФЕРЕ КУЛЬТУРЫ

Сфера культуры занимает особое место в функционировании социума и цивилизации, формируя и сохраняя общественные идеалы (нормы и образцы), коммуникационную среду (язык), социальную память (культурные ценности).

Всемирная роль культуры и признание трансграничного характера культурных ценностей стали одной из предпосылок появления глобального информационного общества.

Объекты культуры – неизбежные жертвы войны, «излюбленная» сфера вандализма, терроризма, корыстных противоправных деяний. Именно культура является полем информационного противоборства государств, цивилизационных войн. Как отмечено на октябрьском (2013 г.) заседании Совета по культуре и искусству при Президенте Российской Федерации, − культура – важнейший фактор нашей национальной безопасности [1]. Из Доктрины информационной безопасности Российской Федерации следует, что основным видом сообщений, составляющих объект национальных интересов в информационной сфере, являются сообщения о национальных культурных ценностях [2, с. 130].

Сфера культуры − культурные ценности, учреждения культуры, система управления, информационные активы подвергаются многочисленным угрозам и рискам внутреннего и внешнего характера. Содержание угроз безопасности сообщений, относящихся к культурным ценностям, заключается в возможности

дезорганизации и разрушении системы накопления и сохранения документов, составляющих культурные ценности. По мере роста масштаба и значимости информационных активов, резко возрастают угрозы нарушения их информационной безопасности: целостности, доступности, а также конфиденциальности и правомерного использования. Для демонстрации способности государства и учреждений культуры защищать свои информационные интересы и активы в сфере культуры настоятельно требуется создание полномасштабной системы информационной безопасности.

Проблемная ситуация в области информационной безопасности сферы культуры [3, с. 46] характеризуется, в частности, следующим:

отсутствует концепция и стратегия информационной безопасности сферы культуры;

отсутствует нормативно-правовая база информационной безопасности;

не определены модели нарушителя информационной безопасности;

не выявлены угрозы информационной безопасности;

не оценены риски информационной безопасности;

не определены политики информационной безопасности на ведомственном и организационном уровне.

Среди задач, решаемых в области информационной безопасности сферы культуры можно выделить:

разработка концептуальных документов в области информационной безопасности сферы культуры и нормативно-правовой базы;

обеспечение информационной безопасности культурного наследия Российской Федерации;

обеспечение безопасности цифрового наследия и других информационных активов сферы культуры;

обеспечение всеобщей доступности цифрового наследия;

обеспечение конфиденциальности информации, связанной с авторским правом;

обеспечение конфиденциальности информации, связанной с безопасностью учреждений культуры и персональными данными, которые они собирают;

научно-методическое и кадровое обеспечение информационной безопасности сферы культуры.

Одной из центральных проблем регулирования сферы культуры и обеспечения ее безопасности является создание системы управления информационными активами и рисками в данной области.

В работе [4, с. 29] обозначены следующие цели государства в области управления информационными активами (ресурсами):

создание первичных и производных информационных массивов и продуктов, необходимых для выполнения всего комплекса задач государственного управления и реализации конституционных прав граждан на доступ к информации;

надежное хранение и защита информационных активов;

эффективное использование информационных активов в деятельности органов власти и государственных учреждений;

обеспечение свободного доступа граждан и организаций к информационным активам в соответствии с Конституцией и действующим законодательством Российской Федерации.

В сфере культуры можно выделить три области обеспечения безопасности информационных активов:

обеспечение информационной безопасности активов, влияющих на безопасность культурного наследия;

обеспечение безопасности информационных активов как части культурного наследия;

обеспечение безопасности информационных активов сферы культуры как отрасли народного хозяйства.

Для принятия решений в области развития культуры, ее информатизации, обеспечении информационной безопасности необходима оценка значимости информационных активов сферы культуры, опирающаяся на их инвентаризацию [5, с. 50].

Оценка значимости информационных активов зависит от оценки культурных ценностей, но данная зависимость не является «линейной». Сама оценка значимости (историческая, стоимостная, иная) культурных ценностей является сложным и неоднозначным процессом, зависящим от множества исторических, религиозных, идеологических, социально-экономических, финансовых и иных факторов [6, с. 20]. Оценка значимости информационной составляющей культуры, в которой представлены информационные образы объектов культуры, и связанные с этим информационные системы, является новой и малоисследованной проблемой.

Приведем пример методики оценки значимости информационного актива (объекта цифрового наследия) как совокупности оценок культурной ценности (культурного актива) и самого цифрового материала.

$$УЗ\ ОЦН = [УЗ_{КЦ}\ УЗ_{ЦМ}]$$

Критерии оценки цифрового материала включают: аутентичность и достоверность, тип цифрового материала, параметры цифрового качества, алгоритм и степень сжатия материала, возможность повторенного получения цифрового образа, другие критерии. Данные критерии позволяют оценивать $УЗ_{ЦМ}$, который мы проводим здесь в шкале 1-5. В Табл. 1 приводится схема оценки, а в Табл. 2 приведены уровни значимости объекта цифрового наследия в зависимости от уровня значимости (масштаба) культурной ценности – мирового, национального, регионального или местного уровня.

Таблица 1. Схема оценки цифрового объекта в условиях наличия/утраты исходного объекта или его аналогового образа

Объект	**Наличие/отсутствие объекта**

Исходный	+	+	+	–	–	–
Аналоговый образ	+	+	–	+	–	–
Цифровой	+	–	–	+	+	–
Оценка ОЦН	низкая	умеренная	средняя	высокая	высшая	–

Таблица 2. Уровни значимости объекта цифрового наследия

	УЗ кц			
УЗ цн	**Мировой**	**Национальный**	**Региональный**	**Местный**
5	высший (УЗ_ОЦН_5)	высший	высокий	средний
4	высокий (УЗ_ОЦН_4)	высокий	средний	умеренный
3	средний (УЗ_ОЦН_3)	умеренный	низкий	низкий
2	умеренный (УЗ_ОЦН_2)	низкий	низкий	низкий
1	низкий (УЗ_ОЦН_1)	низкий	низкий	низкий

Такой подход к комплексной оценке уровня значимости информационного актива в сфере культуры соответствует подходу, определенному в приказе ФСТЭК от 11 февраля 2013 г. N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [7]. В данном приказе приведена формула расчета уровня значимости информации. Этот уровень определяется степенью возможного ущерба для обладателя информации от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации.

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)], где степень возможного ущерба определяется обладателем информации самостоятельно, экспертным или иными методами.

В результате по уровням значимости, приведенным в табл.2., мы можем определять классы защищенности информационных систем в сфере культуры, содержащих информационные активы соответствующего уровня значимости.

Как культурные ценности группируются в коллекции, собрания, фонды, так и информационные активы могут группироваться в портфели активов, требующих своих методов оценки и методов управления, в частности, управления рисками.

Культурные ценности, а также объекты управления, законодательно относящиеся к сфере культуры, чрезвычайно многообразны и простираются от языков народов России до животных в цирках и зоопарках. Поэтому задача идентификации, классификации и ранжирования угроз [8] в сфере культуры

является чрезвычайно многоплановой и сложной. Эта многоплановость и сложность неизбежно отразится в спектре вызовов и задач, стоящих перед обеспечением безопасности информационных активов в сфере культуры.

Принципиально новые угрозы культуре и ее информационным активам возникают в связи с изменением антропологической и ноосферной ситуации, складывающейся в связи с развитием глобальных социальных сетей и виртуальных личностей [9, с.5; 10, с. 42].

«Естественно-консервативное» профессиональное культурное сообщество, основанное на людях с гуманитарным складом мышления и образования, пока плохо воспринимает технические инновации даже в области маркировки музейных предметов. Необходимая регламентация деятельности, связанная с обеспечением информационной безопасности, пока будет вызывать определенное отторжение и непонимание. Справедливости ради следует отметить, что и специалисты в области ИКТ и ИБ, зачастую не видят, или не хотят видеть специфики задач, стоящих перед информатизацией и информационной безопасностью в сфере культуры.

Творческая и кропотливая работа предстоит и в области разработки нормативно-правовой базы информационной безопасности в сфере культуры. Здесь требуется соединение выработанных веками подходов к сохранению культурных ценностей с современными подходами к методам, методикам, стандартам, политикам и процедурам информационной безопасности [11].

В настоящее время по заказу Министерства культуры Российской Федерации при участии авторов настоящей работы разрабатывается следующий комплекс документов:

- «Концепция информационной безопасности»,
- «Комплект политик ИБ»,
- «Методика оценки информационных активов»,
- «Модели угроз и рисков ИБ»,
- «Методики оценки угроз и рисков ИБ»,
- «Методика оценки уязвимостей информационных систем»,
- «Меры обеспечения ИБ информационных систем и ресурсов»,
- «Методика оценки эффективности системы обеспечения ИБ»,
- «Дорожная карта реализации мероприятий по обеспечению ИБ».

Разработка инструментария системы обеспечения информационной безопасности в сфере культуры является задачей, решение которой необходимо рассматривать в неразрывной связи с вопросами сохранения и доступности культурного наследия Российской Федерации.

В результате создания системы информационной безопасности на основе разрабатываемого инструментария:

увеличиться сохранность и доступность культурных ценностей;

повысится упорядоченность и возрастет качество информационных активов;

возрастет защищенность информационных систем и активов как части культурного наследия;

будут обеспечены меры информационной безопасности сферы культуры как отрасли.

ЛИТЕРАТУРА.

1. Заседание Совета по культуре и искусству при Президенте Российской Федерации [электронный ресурс]. URL:http://state.kremlin.ru/face/19353 (дата обращения 22.02.2014).
2. *Стрельцов А.А.* Правовое обеспечение информационной безопасности России: теоретические и методические основы. — Минск: Беллітфонд, 2005. — 304 с.
3. *Кондратьев Д.В., Ненашев А.Н., Петров С.Т., Тарасов А.А.* Проблемы сохранения цифрового культурного наследия в контексте информационной безопасности. // *Вестник РГГУ. Серия Информатика. Защита информации. Математика*. — 2013. — № 14(135). — С. 36-52.
4. *Антопольский А.Б.* Информационные ресурсы России — М.: «НТЦ Информрегистр», 2002. — 330 с.
5. *Зенкевич В., Шатов В.* Информационные риски: анализ и количественная оценка // *Бухгалтерия и банки*. — 2007. — № 1. — С. 50-53.
6. *Шестаков В.А.* Комплексная концепция музейной безопасности — Спб.: АНО НИИ СМД, 2013. — 199 с.
7. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. N 17 г. Москва // Российская газета. — 2013. — № 6112 от 26 июня 2013 г..
8. *Кордонский С.Г.* Классификация и ранжирование угроз. // *Отечественные записки*. — 2013. — № 2 (53). — С. 52-73.
9. *Петров С.Т., Расторгуев С.П.* Компьютеризация и витализация окружающего мира // Информационные войны, 2014. № 2.
10. *Шмидт Э. Коэн Дж.* Новый цифровой мир. Как технологии меняют жизнь людей, модели бизнеса и понятие государств. / пер. с англ. Сергея Филина — М.: Манн, Иванов и Фарбер, 2013. — 368 с.
11. *В. В. Андрианов С. Л. Зефиров В. Б. Голованов Н. А. и др.* Обеспечение информационной безопасности бизнеса. — 2-изд. — М.: Альпина Паблишер, 2011. — 392 с.