

**ЦИФРОВЫЕ КОПИИ МУЗЕЙНЫХ ОБЪЕКТОВ И ОБЕСПЕЧЕНИЕ
ИХ СОХРАННОСТИ: ОПЫТ ГОСУДАРСТВЕННОГО
ГЕОЛОГИЧЕСКОГО МУЗЕЯ ИМ. В. И. ВЕРНАДСКОГО**

ИВАН НИКОЛАЕВИЧ ГАВРЮШИН

Государственный геологический музей им. В. И. Вернадского

Россия, 125009, Москва, ул. Моховая, д. 11, стр. 11

E-mail: i.gavryushin@sgm.ru

Статья очерчивает основные причины и необходимость сохранения исторической памяти о музейном пространстве и экспонатах музея в разные периоды и предлагает ряд технических приемов для организации защиты музейных объектов. Автор ставит своей целью обратить внимание научного сообщества на необходимость разработки новой концепции защиты цифровой информации в научных и культурных организациях, а также предлагает методику, опробованную в последние десятилетия для хранения и распространения программного обеспечения в мире UNIX-подобных операционных систем.

Ключевые слова: музейное дело, информатика в музейном деле, культура знания, защита цифровых объектов научного и культурного значения, защита информации.

DOI: 10.7868/S020596061802009X

**DIGITAL COPIES OF MUSEUM OBJECTS AND THEIR
PRESERVATION AT THE V. I. VERNADSKY STATE GEOLOGICAL
MUSEUM**

IVAN NIKOLAEVICH GAVRYUSHIN

V. I. Vernadsky State Geological Museum

Ul. Mokhovaya, 11, str. 11, Moscow, 125009, Russia

E-mail: i.gavryushin@sgm.ru

The paper outlines the main reasons for preserving historical memory of the museum space and exhibits during different periods and offers a number of technical approaches to museum objects preservation. The author seeks to draw attract attention of the

scientific community to the necessity of developing a new concept of protecting digital information at science and culture organizations and proposes a proven methodology for storing and distributing software in the world of UNIX-like OS. This methodology has been tested over the last few decades.

Keywords: museum studies, information technology in museum studies, knowledge culture, protection of digital objects of scientific and cultural importance, information protection.

В настоящее время во многих российских музеях имеются виртуальные экспозиции, проводятся виртуальные экскурсии и хранятся цифровые копии различных объектов, имеющих историческую ценность. Под цифровой копией подразумевается трехмерное или двухмерное изображение, хранящееся в электронном виде, которое может быть использовано для полного или частичного воспроизведения утраченного оригинала, например, методом печати на 3D-принтере. Растущая ценность этой цифровой аудиовизуальной информации требует ее защиты, например, от умышленного повреждения или искажения или повреждения в результате выхода из строя средств хранения.

В случае сильного изменения физического оригинала или его утраты цифровая копия может оказаться единственным источником, по которому в будущем можно будет полностью или частично воссоздать физическую копию утраченного экспоната. Выполнение такой задачи — реконструкции памятника по цифровой копии — может потребоваться сугубо в научных, научно-исторических, образовательных, экспозиционных или в иных целях. В связи с этим важнейшим элементом защиты данных, представляющих научную или историческую ценность, от фальсификации и повреждения является организация проверки целостности цифровых копий предметов.

В настоящей статье представлен подход к организации защиты цифровых копий экспонатов, практикуемый в Государственном геологическом музее им. В. И. Вернадского. Здесь был предложен следующий подход к организации проверки их целостности:

- для загруженного на сервер цифрового файла генерируется сумма хеширования по общеизвестному алгоритму, например, md5, sha256 или по алгоритму государственного стандарта, например, ГОСТ 34.11-2012, именуемому в Интернете «Стрибогом»;

- порядковый номер, инвентарный номер, название предмета и сумма хеширования сохраняются на сервере, цифровом или бумажном носителе.

В случае выявления уязвимостей в алгоритмах хеширования и их устаревания с течением времени предлагается осуществлять хеширование дополнительными алгоритмами, которые будут разработаны в будущем и будут соответствовать уровню безопасности своего времени. Новые суммы хеширования предлагается добавлять к старым, на независимый носитель, хранящий базу данных. Необходимо указать, что такой механизм при добавлении нового алгоритма позволит периодически, но не слишком часто, проверять состояние данных и автоматически находить проблемные записи. После или

во время проверки целостности данных устаревшие алгоритмы могут быть заменены более новыми.

Таким образом, можно в будущем обеспечить преемственность хеширующих алгоритмов и поддерживать систему проверки подлинности в актуальном состоянии. Устаревшая база данных с устаревшими алгоритмами хеширования после проверки может быть переведена в «глубокое» архивное состояние и какое-то время храниться на твердотельных или дисковых носителях. Во временной перспективе можно обеспечить ротацию баз данных при накоплении достаточного количества обновлений алгоритмов хеширования для одной базы.

Напомним об общих проблемах алгоритмов хеширования и путях их решения: известно, что изменение цифровой копии и генерация суммы хеширования в крайне редких случаях может привести к коллизиям, когда файл изменился, а новая сумма хеширования совпала с предыдущей. Для избежания этой проблемы при архивации особо ценных данных может быть задействован дополнительный алгоритм генерации суммы хеширования, что должно практически исключить возможность подобных коллизий.

Таким образом, для данных, имеющих различную ценность, могут быть предложены разные уровни проверки подлинности, где уровень может определяться, например, количеством используемых алгоритмов.

Важно помнить о том, что цифровую копию можно создать для практически любого объекта научно-исторического или культурного наследия: фотография образца минерала, как в минералогическом музее, рукопись известного ученого, книга или же иной важный документ, который в случае утраты оригинала остается в единственном экземпляре — цифровом.

Проблема проверки целостности информации и организации хранения хешируемых данных в настоящий момент волнует специалистов совершенно разных профилей. Например, тему актуальности данных вопросов в автореферате к своей диссертации И. Ю. Нураев начинает с описания проблемы, которая совершенно очевидно совпадает с описанной в данной статье проблематикой.

Объективный контроль целостности информации чрезвычайно важен для национальной безопасности, работы гражданских институтов, связи и управления, сохранности научной и технической информации. Более 90 % компаний сталкиваются с внутренними вторжениями, 78 % инсайдерских нарушений целостности данных держатели скрывают, а пользователи не имеют возможности доказать факты таких нарушений.

Контроль целостности данных в условиях возможности злонамеренных действий (искажения, удаления, замены информации), особенно действий с санкционированным доступом к базам данных и каналам связи, остается, к сожалению, нерешенной задачей ¹.

¹ Нураев И. Ю. Метод и алгоритмы контроля целостности конфиденциальных данных на основе функций хеширования. Автореферат дис. ... кандидата технических наук. М., 2013. С. 1.

Надо отметить, что автор данной статьи совершенно независимо столкнулся с теми же проблемами безопасности в результате сотрудничества с несколькими российскими музеями. Это стало основанием для вывода, что в настоящее время автоматизированные системы учета музейных предметов не используют системы проверки подлинности цифровых копий, так как время применения таких систем в музеях имеет относительно небольшой срок, а данная возможность просто не закладывалась в самые распространенные системы учета, используемые в настоящее время в музеях Российской Федерации. Однако с учетом постоянно растущего объема единиц хранения российских музеев и периодической утратой — полной или частичной — различных экспонатов по естественным причинам или вследствие действия непреодолимых сил через неопределенное количество времени множество цифровых копий могут оказаться единственным достоверным источником знания о существовании того или иного предмета.

Внедрение систем проверки подлинности в музеях является частью борьбы за сохранение исторической памяти, культурного и научного наследия².

В связи с вышесказанным необходимо выделить ряд дальнейших задач, требующих своего решения:

- передача данных о наиболее ценных экспонатах или обо всех экспонатах с их суммами хеширования на хранение в специализированную независимую организацию;

- создание центра хранения указанных данных (или же поднятие вопроса о возможности использования существующих государственных структур для передачи в них данных о цифровых копиях с их суммами хеширования);

- выработка механизма обновления данных в случае замены цифровой копии, например, при повторной оцифровке экспоната.

References

- Nuraev, I. Iu. (2013) *Metod i algoritmy kontrolya tselostnosti konfidentsial'nykh dannykh na osnove funktsii kheshirovaniia. Avtoreferat dis. ... kandidata tekhnicheskikh nauk [Method and Algorithms for Confidential Data Integrity Control Based on Hash Functions. Abstract of the Thesis for the Candidate of Technical Sciences Degree]*. Moskva.
- Kudrina, E. L. (ed.) (2009) *Globalizatsiia i puti sokhraneniia traditsionnoi kul'tury: sbornik statei Mezhdunarodnoi nauchno-prakticheskoi konferentsii (g. Kemerovo, 16 noiabria 2009 goda) [Globalization and Methods of Traditional Culture Preservation: A Collection of Papers of the International Conference (Kemerovo, 16 November 2009)]*. Kemerovo: Kemerovskii gosudarstvennyi universitet kul'tury i iskusstv, 2009.

² Глобализация и пути сохранения традиционной культуры: сборник статей Международной научно-практической конференции (г. Кемерово, 16 ноября 2009 года) / Отв. ред. Е. Л. Кудрина. Кемерово: Кемеровский государственный университет культуры и искусств, 2009.