Педагогические науки

УДК 004

Р.Х. Багдасарян

Е.С. Лосева

А.Е. Сергеев

Багдасарян Рафаэль Хачикович, кандидат технических наук, доцент кафедры библиотечно-библиографической деятельности и информационных технологий Краснодарского государственного института культуры (Краснодар, ул. им. 40-летия Победы, 33), e-mail: rafael_555@mail.ru

Лосева Екатерина Сергеевна, студентка 4 курса группы Док/бак-18 ИБФ Краснодарского государственного института культуры (Краснодар, ул. им. 40-летия Победы, 33), e-mail: katyhka-losewa@mail.ru

Сергеев Александр Евгеньевич, студент 2 курса группы Бид/маг-20 ИБФ Краснодарского государственного института культуры (Краснодар, ул. им. 40-летия Победы, 33), e-mail: alex_serg88@bk.ru

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СФЕРЕ БИБЛИОТЕЧНОЙ ДЕЯТЕЛЬНОСТИ

Статья посвящена проблемам защиты информации в библиотечной деятельности. В ней исследуются основные термины в области информационной безопасности, выявляются существующие угрозы целостности, конфиденциальности и доступности информации. В статье предлагаются комплексные меры по защите данных, а также правила построения эффективной политики безопасности в библиотечной деятельности.

Ключевые слова: библиотечная деятельность, информация, информационная безопасность, библиотека, защита информации.

R.Kh. Bagdasaryan

E.S. Loseva

A.E. Sergeev

Bagdasaryan Rafael Khachikovich, candidate of technical sciences, associate professor of department of library and bibliographic activity and information technologies of the Krasnodar state institute of culture (33, im. 40-letiya Pobedy st., Krasnodar), e-mail: rafael_555@mail.ru

Loseva Ekaterina Sergeevna, 4th course student of Doc/bak-18 IBF group of the Krasnodar state institute of culture (33, im. 40-letiya Pobedy st., Krasnodar), e-mail: katyhka-losewa@mail.ru

Sergeev Alexander Evgenyevich, 2nd course student of the Bid/mag-20 IBF group of the Krasnodar state institute of culture (33, im. 40-letiya Pobedy st., Krasnodar), e-mail: alex_serg88@bk.ru

INFORMATION SECURITY IN THE FIELD OF LIBRARY ACTIVITY

This article is devoted to the problems of information protection in library activities. It explores the basic terms in the field of information security, identifies existing threats to the integrity, confidentiality and availability of information. The article offers comprehensive data protection measures, as well as rules for building an effective security policy in library activities.

Key words: library activity, information, information security, library, information protection.

В настоящее время информационная безопасность (ИБ) становится одним из важнейших аспектов в различных сферах деятельности, связанных

с большим объемом данных, хранящихся на различных уровнях (государственном, кадровом, отраслевом или международном) [1].

Безопасность информационных ресурсов (ИР), создаваемых и хранящихся в государственных библиотеках, используемых для этого технологий следует рассматривать как одну из приоритетных проблем национальной безопасности любой страны, которая должна быть связана с утвержденной концепцией национального хранилища ИР [2].

Если рассматривать информационную безопасность как защиту данных и поддержку от несанкционированного доступа, который нанесет колоссальный ущерб всем пользователям или владельцам информации, то необходимо искать логический подход с точки зрения решения проблем, касаемых информационной безопасности. С самого начала необходимо определить объект информации и интерес субъектов, которые связаны с использованием этих систем.

К объектам информационной безопасности в сфере деятельности библиотеки относятся различные права и свободы личности, а также духовная и материальная сторона современного общества.

ИБ следует рассматривать как доступ к данным, которые в свою очередь подразделяются на ограниченные (доступные каждому) и закрытые.

Под общедоступными данными следует понимать данные, которые свободно доступны и раскрываются по определенному принципу, такому как все, что не запрещено законом, может использоваться в открытом доступе. Следовательно, открытые данные являются объектами накопления, обработки, анализа и хранения в библиотеках.

ИБ – это комплексный, многомерный вид деятельности, который не ограничивается защитой данных, но имеет более глобальную цель.

Для достижения желаемого результата необходимо использовать комплексный и системный подходы.

В этой связи нельзя не учитывать как интересы субъектов, так и средства защиты информации.

Все интересы субъектов, которые связаны с использованием ИР, можно разделить на следующие свойства:

1. Доступность данных.
2. Целостность данных.
3. Конфиденциальность данных [3].

Наряду с развитием информационной сети, оцифровка и объединение библиотек с информационными ресурсами, безусловно, дает пользователям беспрецедентное удобство и широкое пространство для обучения, что, в свою очередь, приводит к увеличению количества непредвиденных последствий и угроз, связанных с информационной безопасностью библиотек.

Обеспечение соответствующей безопасности используемых в рабочем процессе всех устройств, данных и ИТ-систем в библиотечном процессе, которые не будут повреждены и изменены в результате несанкционированного доступа, в настоящее время стало насущной проблемой современного управления библиотекой.

Информационная безопасность библиотеки для обеспечения конфиденциальности, целостности, доступности, подлинности и управляемости всех данных использует технологии управления сетью.

В настоящее время широко используются межсетевые экраны и виртуальная частная сеть (VPN).

Брандмауэр – это программный или программно-аппаратный элемент компьютерной сети, который отслеживает и фильтрует проходящий через него сетевой трафик на основе определенных правил, которые часто встречаются на узлах в библиотечной сети. Он может контролировать, фильтровать информацию, передаваемую из сети «Интернет» или по локальной сети. VPN в первую очередь позволяет решить проблемы безопасности межрегиональной передачи данных между различными филиалами или системами библиотек по общедоступной сети [4].

Работа и управление сетевым оборудованием системы влияет на безопасность сети, сегментация сети, используемая в данном процессе, позволяет предотвратить угрозы при передаче данных. Если рассматривать вопросы, касаемые информационной безопасности непосредственно самой операционной системы Windows, то здесь требуется своевременная установка исправлений безопасности системы и постоянное обслуживание системы в целом.

В системе для разных пользователей и сотрудников для работы системных файлов и программ необходимо проводить разграничение прав доступа (установка личных паролей), обычно это реализуется посредством доменной сети. В управлении библиотекой, где используется много данных, очень важно, как будет реализовано и технически оснащено нормальное функционирование сети.

Безопасность библиотечной информации заключается в том, что сетевые ИР не были потеряны, изменены, похищены и, в конечном итоге, не стали общедоступными в сети «Интернет».

В глобальной сети компьютерная система в любой момент времени по разным причинам будет подвержена различным угрозам.

Как правило, причина исходит от оборудования или программного обеспечения, она может быть искусственной или вызванной объективными факторами. В любом случае при возникновении такого инцидента необходимо незамедлительно возобновить работу всей системы и обеспечить читателям библиотеки бесперебойный доступ к информации.

Актуальная копия резервных данных служит для обеспечения безопасности и доступности информации в библиотечной системе. Ее присутствие позволяет в решении большинства проблем библиотеки. В связи с чем на этом этапе рекомендуется внимательное отслеживание всех устройств, ответственных за хранение резервной копии. Данный результат возможен при своевременном обновлении программного обеспечения

системы и устройств, лицензионных программных продуктов, в частности, антивирусного приложения.

Во многих библиотечных системах основными элементами информационных систем являются устройства (сервер со своими хранилищами данных), обеспечивающие сбор, передачу и хранение данных. Все технические компоненты, которые используются в соответствии с рекомендациями в ИС библиотеки, должны иметь высокую производительность и надежность. Во избежание потери данных резервное копирование следует делать не реже одного раза в месяц.

Для защиты интересов субъектов действуют нормативно-правовые и административные акты общего характера, конкретные меры безопасности, программные и аппаратные меры, а также меры, направленные на создание и поддержание негативного и даже карательного отношения в компании к противоправным действиям, которые могут применяться к нарушителям ИБ, и прямые (меры координации), которые повышают грамотность всего общества и знания в области информационной безопасности, что в дальнейшем будет способствовать созданию и тиражированию различных программных инструментов для обеспечения информационной безопасности в целом [5].

Законодательство об ИБ включает конституционные положения: о безопасности, о государственных секретах, информации, компьютеризации и защите информации и т. д., гарантирующие правовые основы безопасности общества и личности страны, систему безопасности и ее функциональность, порядок организации различных органов, занимающихся безопасностью, а также контроль и надзор за законностью в сфере информационной безопасности [6].

Можно рассмотреть группы мер, которые будут направлены на обеспечение ИБ:

а) физическая защита;

б) управление персоналом;

в) поддержание работоспособности;

г) реагирование на различные нарушения;

е) разработка и применение плана для восстановления.

Функциональность информационной безопасности должна быть реализована в распределенной среде. Это означает, что программное обеспечение и вычислительные устройства будут соответствовать универсальным стандартам и могут быть устойчивы к различным атакам и угрозам по отношению к сети.

Система ИБ должна обеспечивать защиту этих библиотек и их информационных систем от различных типов чрезвычайных ситуаций, сетевых атак, терроризма, использования оружия, а также угроз, напрямую связанных через сеть «Интернет».

Современная библиотека – это не только источник различных идей, технологий, мыслей, фактов и различных типов данных, опубликованных в виде различных книг, периодических изданий, диссертаций, рукописей и т.д., но и автоматизированная информация [7].

Система центра, имеющая в своей структуре огромный перечень медиатек и доступ в сеть «Интернет», в своей работе использует цифровое аудио- и видеооборудование, спутниковое телевидение, сетевые технологии, чтобы современные библиотеки могли стать распространителями таких данных, которые могут нанести вред личности человека (азартные игры, расистские высказывания, ненормативная лексика, запрещенные наркотические вещества и т.д.).

Нарушение технологической обработки данных впоследствии может привести к проблемам, связанным с безопасностью информации.

Несвоевременная обработка и анализ поступающих данных, сбои, некорректное заполнение полей при вводе данных в информационно-поисковые системы библиотеки становятся препятствием в поиске и приеме данных.

К числу угроз ИБ данных ресурсов информации самим библиотекам следует отнести:

1) Природные катаклизмы.
2) Производственные аварии.
3) Пожары.
4) Террористические акты.
5) Перехват и несанкционированный доступ информации.
6) Кражи.
7) Компьютерные преступления.
8) Использования некачественных продуктов в сфере создания ИР.

Проблема перехвата информации, в т.ч. киберпреступлений, стала особенно острой с повсеместным внедрением современных информационных технологий.

Благодаря использованию технологии электронной доставки файлов документов по электронной почте, а также традиционных средств передачи данных (межбиблиотечный абонемент), проблема перехвата данных стала весьма актуальной, выдвигая безопасность документов на первый план.

К компьютерным преступлениям, наносящим ущерб информационным ресурсам, относятся преступления против конфиденциальности, целостности данных, компьютерных систем и правил доступа к ним.

К ним относятся: незаконный доступ, манипулирование данными, распространение компьютерных вирусов, спам – «электронные отходы».

Сегодня ИБ библиотечной системы – это сложный комплекс мер и различных защитных действий, направленных на исключение потери данных.

Кроме того, современная защита информации должна соответствовать международным корпоративным, национальным, методическим и нормативным стандартам.

На основании вышеизложенного можно сделать вывод, что свобода, процветание и развитие общества и личности относятся к основным человеческим ценностям.

Однако эффективное участие в жизни общества возможно только при условии удовлетворительного образования, а также свободного и неограниченного доступа к знаниям, идеям, культуре и, конечно, данным. Следовательно, информационная безопасность немыслима без надлежащей защиты крупных хранилищ данных и их ИТ и телекоммуникационной инфраструктуры.

Обеспечение информационной безопасности при работе библиотеки является первоочередной задачей различных аспектов информационных отношений, что, в свою очередь, будет невозможно без соблюдения принципов, описанных выше.

Список используемой литературы:

1. Автоматизированная библиотека: достижения, новации, перспективы / Ред.-сост., авт. вступ. ст. Т.В. Майстрович. – М.: Библиотека, 2017. – 479 с.

2. *Гафнер, В. В.* Информационная безопасность: учебное пособие / В.В. Гафнер. – Рн/Д: Феникс, 2017. – 324 с.

3. *Громов, Ю. Ю.* Информационная безопасность и защита информации: учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2017. – 384 с.

4. *Малюк, А. А.* Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. – М.: ГЛТ, 2016. – 280 с.

5. *Партыка, Т. Л.* Информационная безопасность: учебное пособие / Т.Л. Партыка, И.И. Попов. – М.: Форум, 2016. – 432 с.

6. *Петров, С. В.* Информационная безопасность: учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. – М.: АРТА, 2016. – 296 с.

7. *Семененко, В. А.* Информационная безопасность: учебное пособие / В.А. Семененко. – М.: МГИУ, 2017. – 277 с.