ЗАЯВЛЕНИЕ ИФЛА О КИБЕРБЕЗОПАСНОСТИ

IFLA STATEMENT ON CYBERSECURITY*

Программное заявление ИФЛА, подготовленное Секцией информационных технологий, предназначено для библиотек, библиотечных ассоциаций, преподавателей в области библиотечного дела и библиотековедения, а также для правительственных структур (включая межправительственные организации). Документ призван разъяснить концепцию кибербезопасности в контексте работы библиотек, а также дать рекомендации по улучшениям в этой области.

Библиотеки выступают в качестве портала по предоставлению информации, а публичные библиотеки играют все более активную роль в устранении неравенства в доступе к ней. Выполняя эту миссию, библиотеки все больше полагаются на цифровые технологии для обеспечения доступа к информации, а также повышения эффективности собственной работы.

При этом библиотеки сталкиваются с тем фактом, что их системы могут быть уязвимы для атак, имеются риски как для учреждений и персонала, так и для пользователей. Таким образом, кибербезопасность является важным элементом библиотечной работы, направленным на защиту пользователей и сотрудников библиотек в процессе обеспечения общественного доступа к информации.

В связи с этим возрастает потребность в рассмотрении того, каким образом библиотеки могут подходить к проблеме кибербезопасности, чтобы поддерживать ключевые ценности, связанные с интеллектуальной свободой. Это подразумевает свободу беспрепятственно придерживаться своего мнения и искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ (включая свободу чтения и более широкую свободу доступа к информации и свободу выражения мнений), см., в частности, Заявление ИФЛА о неприкосновенности частной жизни в библиотечной среде (2014)[1] и Заявление ИФЛА по поводу библиотек и интеллектуальной свободы (1999)[2].

Кибербезопасность: почему она важна в библиотеках

Понятие кибербезопасности подразумевает защиту сетей, устройств и данных от несанкционированного доступа и/или использования. С этим тесно связаны усилия по обеспечению конфиденциальности, целостности и доступности информации (см.: Агентство по кибербезопасности и инфраструктурной безопасности США[3], Национальный центр кибербезопасности Великобритании[4], Европейское агентство по сетевой и информационной безопасности, ENISA[5]). Некоторые рассматривают это как часть более широкой концепции цифровой безопасности (выходящей за рамки технической и/или криминальной безопасности), чтобы учитывать также экономические и социальные аспекты[6].

Стандарты в области кибербезопасности сосредоточены в следующих компонентах информационных систем:

- критически важные приложения;
- серверы и установки, поддерживающие приложения (центры обработки данных и т. д.);
- безопасность сетей, обеспечивающих работоспособность системы;
- безопасность разработки программного обеспечения, управления изменениями и развертывания;
- конечный пользователь или клиентская среда.

Все это актуально в отношении библиотек и их усилий по обеспечению кибербезопасности, при этом не все библиотеки имеют одинаковый уровень контроля и управления различными компонентами используемых ими систем. Находясь во многих различных институциональных контекстах, политика библиотеки в области кибербезопасности часто определяется общей политикой руководящего учреждения.

Например, библиотеки могут иметь мало полномочий в управлении инфраструктурой, в рамках которой они работают, но, как правило, они участвуют в среде конечного пользователя или клиентской среде и играют решающую роль в выборе, администрировании, обучении и управлении библиотечными системами и предоставляемыми услугами.

Области, затрагивающие библиотечную деятельность, и информационно-пропагандистская работа

Своими действиями или путем влияния на действия других лиц библиотекам предлагается продвигать кибербезопасность в следующих областях:

* https://repository.ifla.org/handle/123456789/1912

• защита библиотечных систем от рисков и угроз кибербезопасности с целью обеспечения постоянного предоставления услуг;

• обеспечение защиты пользователей библиотек от интернет-угроз при использовании библиотечных систем;

• защита конфиденциальности пользовательской информации.

Многие библиотеки, предоставляя доступ в Интернет, также несут юридические или иные обязательства по предотвращению использования этого доступа во вред другим лицам. Таким образом, библиотекам также могут потребоваться усилия для обеспечения того, чтобы сами пользователи, работая с библиотечными системами или ресурсами, не занимались преступной деятельностью в киберпространстве и соблюдали политику учреждений по допустимому использованию сетей.

Однако люди вполне могут пользоваться Интернетом и другими информационными системами за пределами библиотеки, поэтому имеется также возможность поощрять поведение и протоколы для безопасного использования услуг с помощью программ цифровой грамотности. Например, в Стратегии безопасности в сети Интернет Великобритании подчеркивается важность образования[7].

Поиск баланса

Очевидно, что продвижение принципов кибербезопасности является неоднозначным процессом. Усилия по выявлению потенциальных рисков могут вступить в противоречие с усилиями по обеспечению конфиденциальности пользователей библиотеки и других лиц.

Например, библиотеки могут обязать внедрить технологии для обеспечения соблюдения политики приемлемого использования или подвергнуть (наряду с пользователями Интернета в более широком смысле) надзору со стороны органов безопасности. В таких случаях важно открыто информировать пользователей о существующих правилах и инструментах, чтобы дать им возможность принять взвешенное решение.

Разумеется, во многих случаях цели стратегий кибербезопасности и соблюдения конфиденциальности могут совпадать. Например, риск потери личных данных в результате кибератак возможно свести к минимуму, если библиотеки не будут сохранять ненужные личные данные, а также обеспечат надлежащее шифрование важной информации.

Рекомендации

В связи с этим ИФЛА сформулировала следующие рекомендации. Там, где библиотеки несут ответственность (частичную или полную) за свои собственные информационные системы, они должны:

• внедрять политику по минимизации сбора и хранения данных, включая удаление истории использования по истечении определенного времени;

• применять доступные инструменты для защиты пользователей во время работы с библиотечными системами, включая стандартные меры информационной безопасности, зашифрованные веб-службы, эффективный контроль паролей и веб-сеансов, применение принципа минимальных привилегий[8], в то же время обеспечивая максимальную конфиденциальность;

• внедрять средства контроля безопасности конечных точек на всех рабочих станциях и серверах библиотеки (ряд стандартов ISO охватывает вопросы, связанные с кибербезопасностью, однако эти стандарты не выложены в открытом доступе и поэтому не могут быть одобрены ИФЛА в качестве моделей для глобальной библиотечной сферы; примеры включают требования стандарта ISO 27001 — Системы обеспечения информационной безопасности; ISO 27002 — Свод норм и правил применения мер обеспечения информационной безопасности; ISO 27032 — Информационные технологии — Методы обеспечения безопасности — Руководящие указания по кибербезопасности);

• там, где внедрены инструменты для мониторинга ненадлежащего использования или непреднамеренных угроз, действовать так, чтобы обеспечить максимальную прозрачность и уважение конфиденциальности.

В случаях, когда библиотеки являются частью более крупных учреждений (и поэтому не имеют контроля над ключевыми компонентами информационных систем) или вынуждены полагаться на сторонних поставщиков, им следует:

• выступать за эффективные меры соблюдения кибербезопасности со стороны хозяйствующих учреждений, которые также придерживаются принципов конфиденциальности; это может включать продвижение методов, обеспечивающих конфиденциальность при сборе и хранении данных;

• побуждать сторонних поставщиков к внедрению эффективной системы кибербезопасности в библиотеках, чтобы оградить пользователей от неприемлемых рисков при использовании их услуг.

Все библиотеки самостоятельно или в партнерстве с хозяйствующим учреждением (в зависимости от обстоятельств) должны:

• разработать и опубликовать политику допустимого использования при работе в Интернете и с другими информационными системами; политику конфиденциальности, определяющую, где и какая информация собирается, как используется, что происходит в случае нарушения защиты; политику в области кибербезопасности и

информационной безопасности, определяющую принципы и методы, используемые для защиты библиотечных систем и обеспечения устойчивости и восстановления в случае сбоя; это должно основываться на институциональной политике и соответствующих процедурах;

- удостовериться, что весь библиотечный персонал способен применять знания основ кибербезопасности, относящихся к их профессиональным задачам (например, надлежащую практику использования паролей и т. д.);
- изучить потенциал повышения цифровой грамотности среди пользователей, включая понимание того, как избежать угроз кибербезопасности.

Библиотечные ассоциации и другие организации по поддержке должны:

- предоставлять обновления и соответствующую информацию о кибербезопасности в работе библиотек и предлагать, где это возможно, обучение или ссылки на другие ресурсы;
- рассмотреть возможности для сотрудничества с лицами, участвующими в оказании помощи при обеспечении безопасности пользователей в Интернете.

Правительства должны:

- удостовериться, что библиотеки располагают ресурсами и профессиональной подготовкой для максимально полного соблюдения протоколов кибербезопасности, а также инвестировать средства в программы цифровой грамотности (в том числе через библиотеки) в целях повышения безопасности в Интернете[9];
- убедиться, что более широкая политика в области кибербезопасности сочетает эффективность с уважением прав человека, включая неприкосновенность частной жизни.

Приложение: Стандарты ISO

Стандарты ISO представляют общий набор стандартов для кибер- и информационной безопасности в любой организации. Данные стандарты призваны служить основой для норм и правил использования информационных технологий в технических аспектах кибербезопасности в библиотеке.

Стандарт ISO/IEC 27001 (Системы обеспечения информационной безопасности — Требования) определяет требования к четко определенной Системе управления информационной безопасностью (ISMS) в организации. Здесь рассматриваются систематические процессы управления безопасностью[10].

Стандарт ISO/IEC 27002 (Свод норм и правил управления информационной безопасностью) содержит руководящие принципы и рекомендации по передовым практикам для 10 ключевых областей безопасности: политика безопасности; организация информационной безопасности; управление активами; безопасность человеческих ресурсов; физическая и экологическая безопасность; управление коммуникациями и операционной деятельностью; управление доступом; приобретение, разработка и обслуживание информационных систем; менеджмент инцидента информационной безопасности; управление непрерывностью бизнеса и соответствие требованиям. Обычно это относится к области управления безопасностью информационных систем в архитектуре информационных технологий[11].

Стандарт ISO/IEC 27032 (Информационные технологии — Методы обеспечения безопасности — Руководящие указания по кибербезопасности) расширяет базовые методы обеспечения кибербезопасности[12].

Утверждено Правлением ИФЛА,
февраль 2022 г.

Примечания

1 https://www.ifla.org/wp-content/uploads/2019/05/assets/hq/news/documents/ifla-statement-on-privacy-in-the-library-environment.pdf (дата обращения: 11.10.2022)
2 https://ifap.ru/ofdocs/ifla/libif.htm (дата обращения: 11.10.2022).
3 https://us-cert.cisa.gov/ncas/tips/ST04-001 (дата обращения: 11.10.2022).
4 https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security (дата обращения: 11.10.2022).
5 https://www.enisa.europa.eu/publications/definition-of-cybersecurity (дата обращения: 11.10.2022).
6 https://www.oecd.org/digital/ieconomy/digital-security/ (дата обращения: 11.10.2022).
7 https://www.gov.uk/government/consultations/internet-safety-strategy-green-paper (дата обращения: 11.10.2022).
8 https://en.wikipedia.org/wiki/Principle_of_least_privilege (дата обращения: 11.10.2022).
9 https://ieeexplore.ieee.org/document/9092330 (дата обращения: 11.10.2022).
10 https://www.iso.org/standard/54534.html (дата обращения: 11.10.2022).
11 https://www.iso.org/standard/54533.html (дата обращения: 11.10.2022).
12 https://www.iso.org/standard/44375.html (дата обращения: 11.10.2022).

Перевод **Натальи Осецкой**,
Российская государственная библиотека