Аксёнов А.Е., магистрант
дневной формы обучения
Научный руководитель – Яцевич Н.А.,
кандидат педагогических наук, доцент

К ВОПРОСУ О РАЗРАБОТКЕ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКАНСКОЙ НАУЧНОЙ БИБЛИОТЕКИ

Развитие информационных технологий и массовая цифровизация значительно улучшили информационный сервис библиотек, однако привнесли множество новых проблем и угроз, относящихся к конфиденциальности данных, сохранению их целостности и доступности. Защита информации и конфиденциальность данных в библиотеке являются неотъемлемой частью успешного функционирования библиотеки. Библиотека является центром обмена информацией, поэтому необходимо, чтобы все данные и информация, хранящиеся и передаваемые в библиотеке, были защищены от несанкционированного доступа. Кроме того, согласно принятому в 2021 Закону Республики Беларусь “О защите персональных данных” [3], остро встаёт вопрос об организации и внедрении комплекса мер и средств, обеспечивающих конфиденциальность персональных данных пользователей, а также защиту от нежелательных или несанкционированных действий в отношении информационных ресурсов библиотеки.

Существует множество определений информационной безопасности, однако все они, как правило, сводятся к тому, что в основе информационной безопасности лежит деятельность по защите информации, обеспечению её конфиденциальности, целостности и доступности. Информационная безопасность − это также практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения или уничтожения информации.

Для обеспечения защиты информации и информационных ресурсов и в соответствии с приказом Оперативно-аналитического центра (ОАЦ) при

Президенте Республики Беларусь № 66 от 20 февраля 2020 г. [5], библиотека должна разработать и внедрить ***политику информационной безопасности.*** В современной практике термин «политика безопасности» может употребляться как в широком, так и в узком смысле слова. В широком смысле политика безопасности определяется как система документированных управленческих решений по обеспечению безопасности организации. В узком смысле под политикой безопасности обычно понимают локальный нормативный документ, определяющий требования безопасности, систему мер, либо порядок действий, а также ответственность сотрудников организации и механизмы контроля для определенной области обеспечения безопасности.

Примерами таких документов могут служить: политики выбора и использования паролей, установки и обновления программного обеспечения; разработанные и утвержденные правила работы пользователей в корпоративной сети библиотеки и интернете; соглашение о соблюдении режима информационной безопасности и другие нормативные документы. Их общая цель − обеспечение целостности, доступности и конфиденциальности данных, а также их полноты и актуальности.

К примеру, целями политики информационной безопасности в Национальной библиотеке Беларуси являются:

- защита активов от возможного нанесения им материального, физического, морального или иного ущерба посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи;
- соблюдение требований законодательства Республики Беларусь в области защиты информации;
- снижение уровня рисков информационной безопасности и реального ущерба от инцидентов информационной безопасности;
- эффективное управление рабочими процессами (бизнес-процессами), в том числе в критических ситуациях [4].

Большинство библиотек в том или ином виде преследует данные цели и без внедрения политики безопасности. К примеру, БелСХБ не имеет полноценной утверждённой политики информационной безопасности, однако в работу библиотеки внедрена политика паролей и антивирусная политика, разработаны правила работы в локальной сети. Но очевидно, что нельзя обеспечить необходимый уровень защиты данных, реализуя мероприятия по информационной безопасности бессистемно.

Планируя разработку политики информационной безопасности в библиотеке, необходимо руководствоваться приказом ОАЦ № 66 и законом № 99-З «О защите персональных данных» [3], а также другими юридическими и нормативно-техническими документами, так как на их основе выбираются методы и средства для защиты информационных ресурсов библиотеки.

Разработке и внедрению политики информационной безопасности в библиотеке должна предшествовать оценка ее текущего состояния, что осуществляется с помощью аудита − он позволяет оценить и спрогнозировать риски, управлять их влиянием на все информационные активы библиотеки. Важными целями аудита являются определение узких мест в системе защиты информации, а также выработка рекомендаций по внедрению новых и совершенствованию существующих механизмов её защиты.

На основе полученного аудиторного отчёта разрабатывается ***концепция информационной безопасности библиотеки*** − документ, который системно представляет все основные аспекты информационной безопасности конкретной библиотеки и базируется на действующем законодательстве Республики Беларусь, государственных и международных стандартах, методах и средствах обеспечения информационной безопасности, морально-этических нормах, организационных и финансовых возможностях. Концепция является методологической основой формирования и реализации единой политики в области информационной безопасности библиотеки, и также служит основной для принятия управленческих решений и разработки практических мер по ее реализации.

Политика информационной безопасности разрабатывается в соответствии с ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью» [1] и подразделяется на уровни:

К *верхнему* уровню относятся документы, затрагивающие деятельность библиотеки в целом (концепция информационной безопасности, политика информационной безопасности).

К *среднему* уровню относят документы, касающиеся отдельных аспектов информационной безопасности. Это требования на создание и эксплуатацию средств защиты информации, организацию информационных процессов библиотеки по конкретному направлению защиты информации: безопасности баз данных, безопасности коммуникаций, использования криптографической защиты, контент-фильтрации сайтов интернета, использовании электронной подписи и т. п.

На *нижнем* уровне находятся документы, которые определяют процедуры и правила достижения целей и решения задач информационной безопасности и детализирует (регламентирует) эти правила. В политику информационной безопасности этого уровня входят регламенты работ, руководства по администрированию, инструкции по эксплуатации отдельных сервисов информационной безопасности, руководства пользователя.

Таким образом, *организационную* основу реализации политики информационной безопасности библиотеки составляют регламентирующие документы.

Качественная проработка всех уровней политики информационной безопасности − это трудоёмкий и сложный процесс, однако благодаря ей можно найти оптимальный баланс между доступностью и удобством работы с информацией и её защитой. Разработка и внедрение политики информационной безопасности в научные библиотеки позволит обеспечить защиту информационных ресурсов от внешних и внутренних угроз и их оптимальное и безопасное формирование, создание и использование.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Информационная технология. Практические правила управления информационной безопасностью [Электронный ресурс] – Режим доступа: https://docs.cntd.ru/document/1200044724 – Дата доступа: 27.02.2023.

2. Карауш, А. С. Сервер – под замок, или как минимизировать риски [Электронный ресурс] / А. С. Карауш // Библ. дело. – 2007. – №. 2 (50). – Режим доступа: http://www.bibliograf.ru/issues/2007/2/66/0/655/ – Дата доступа: 13.09.2023.

3. О защите персональных данных [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=12551&p0=H12100099&p1=1 – Дата доступа: 28.02.2023.

4. Политика информационной безопасности [Электронный ресурс] – Режим доступа: https://www.nlb.by/content/o-biblioteke/politika-informatsionnoy-bezopasnosti/ – Дата доступа: 24.02.2023.

5. ПОЛОЖЕНИЕ о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2020%20-%2066.pdf – Дата доступа: 24.01.2023.

6. Свергунова, Н. М. Информационная безопасность библиотек [Электронный ресурс] / Н. М. Свергунова // Научная библиотека Орловского государственного университета имени И. С. Тургенева : сайт. – Режим доступа: http://library.oreluniver.ru/docs/publ_sotr/Informacionnay%20bezopasnosti.pdf – Дата доступа: 13.01.2023.